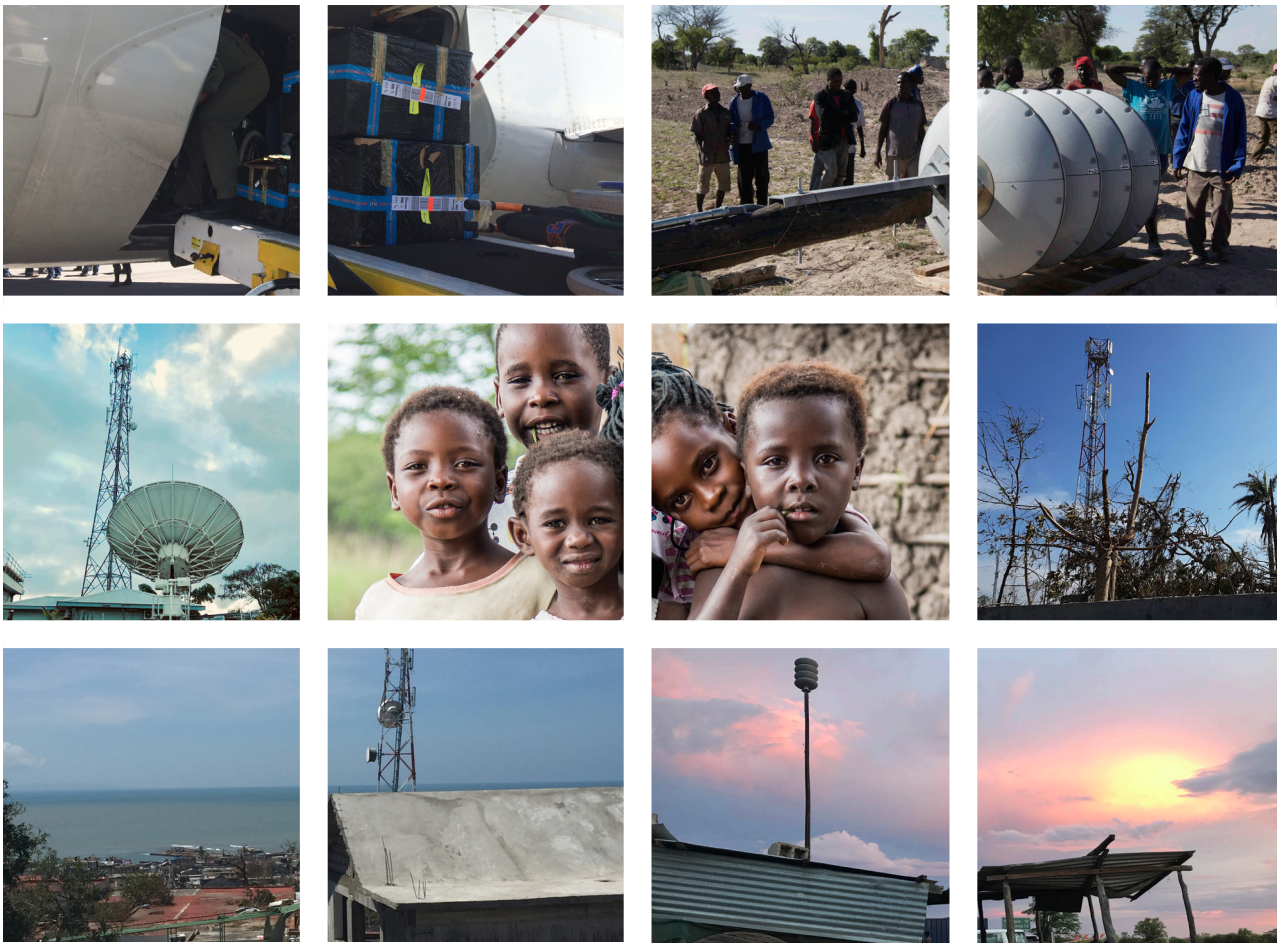
ITUPublications

ITU Guidelines for national emergency telecommunication plans



ITU Guidelines for national emergency telecommunication plans

Acknowledgments

This report was prepared by the International Telecommunication Union (ITU) expert Juan Manuel Roldan, President of Luxon Consulting Group, LLC, and research assistant Felipe Ordoñez, under the direction of the Environment and Emergency Telecommunications Division (EET), within the Digital Networks and Society Department of the Telecommunication Development Bureau (BDT).

ITU would like to warmly thank those who contributed to the public consultation for their constructive and fruitful comments for the revisions of the guidelines, in particular, the GVF group represented by David Meltzer, Dulip Tillekeratne from GSMA, Cecil Ameil from SES, Ria Sen from ETC, Joseph Burton from, U.S. Department of State, José Toscano from Intelsat, Aarti Holla from ESOA, Jennifer Manner from EchoStar, and ITU experts Eliot Christian and Don Wallace.

ISBN

978-92-61-31311-1 (Paper version)

978-92-61-31321-0 (Electronic version)

978-92-61-31331-9 (EPUB version)

978-92-61-31341-8 (Mobi version)

Please consider the environment before printing this report.

© ITU 2020

Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited. In any use of this work, there should be no suggestion that ITU endorse any specific organization, products or services. The unauthorized use of the ITU names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

Table of Contents

1. Overview 1
   - 1.1 Scope and structure 1
   - 1.2 Recommendations 2

2. National emergency telecommunication plan: Step by step 4
   - 2.1 Overall risk assessment 4
   - 2.2 Topics to be included in the NETP 4
   - 2.3 Concepts and principles in a draft national plan 6
   - 2.4 NETP drafting process 12

3. National disaster management 15
   - 3.1 Legal and regulatory framework 15
   - 3.2 Administrative structure and governance model 18
   - 3.3 Public–private cooperation, coordination, communication plans 21
   - 3.4 Contingency plans 23
   - 3.5 Definition of roles and identification of contact points 25

4. Telecommunication/ICT legislation and regulation 26
   - 4.1. Legislation 26
   - 4.2. Regulation 26
   - 4.3. Ensuring regulatory flexibility 29

5. Telecommunication/ICTs for emergencies 30
   - 5.1. Vulnerability and risk analysis of telecommunication/ICT networks 30
   - 5.2. Telecommunication/ICT database for emergencies 31
   - 5.3. Early warning systems 31
   - 5.4. Common alerting protocol 34

6. International cooperation and coordination 37
   - 6.1 Emergency telecommunication cluster 37
   - 6.2 International Telecommunication Union 37
   - 6.3 Tampere Convention 38
   - 6.4 United Nations Office for the Coordination of Humanitarian Affairs 39
   - 6.5 United Nations Office for Disaster Risk Reduction 39
   - 6.6 Bilateral agreements 40

7. Development of capacities and drills 41

8. Support for people with specific needs 46

Annex A: Emergency communications checklist 49

Annex B: Types of disasters 67

Annex C: Historical disasters by region 70

Annex D: Additional information on telecommunication/ICTs for emergencies 74

Annex E: Additional information on the Tampere Convention 84

Annex F: Additional information on drills and exercises 86

Annex G: Additional information on ICT to support people with specific needs 87

References 89

Abbreviations 93

Glossary 94

List of tables, figures and boxes

Tables

Table 1: Topics to be included in a national emergency telecommunication plan 5
Table 2: Principles of a national emergency telecommunication plan 7
Table 3: List of government and private stakeholders to include in workshops and interviews 13
Table C1: Disasters over the 50-year period 1968–2017 70

Figures

Figure 1: Topics to be included in a national emergency telecommunication plan 5
Figure 2: Principles of a national emergency telecommunication plan 6
Figure 3: Four phases of disaster management 8
Figure 4: National emergency telecommunication plan step-by-step drafting process 14
Figure 5: National emergency telecommunication development and implementation 15
Figure 6: Four elements of end-to-end, people-centred early warning systems 32
Figure 7: Common alerting protocol 34
Figure 8: Training ladder 43
Figure B1: Disaster categories according to CRED 67
Figure D1: FEMA Mobile App 77
Figure D2: Satellite systems 78

Boxes

Box 1: SAFECOM Writing Guide for Standard Operating Procedures 16
Box 2: The Colombia administrative structure and governance model 18
Box 3: The United Kingdom administrative structure and organizational model 20
Box 4: The Chile regulations on telecommunication networks for emergency management 22
Box 5: Contingency plans for Covid-19 24
Box 6: Regulations for telecommunication services during emergency situations in Peru 28
Box 7: The Butaleja district in Eastern Uganda: Flood early warning systems 33
Box 8: Common alerting protocol 35
Box 9: NetHope 44
Box 10: Earthquake drills 44
Box 11: gear.UP 45
Box 12: Wireless Emergency Alerts 47
Box 13: PLUSVoice 48
Box 14: Get Ready Get Through 48
Box D1: United States Federal Emergency Management Agency Mobile App 77

1. Overview

The implementation of a national emergency telecommunication plan (NETP) is an essential prerequisite for policy, procedures, and governance that enable reliable and resilient information and communications in all four phases of disaster risk management: mitigation, preparedness, response and recovery.

The effective management of the risk of disasters depends on communication and information sharing across all levels of government, within communities, and between public and private organizations. In particular, timely and effective information flow is important for early warning and alerting the population, for preparing for an emergency event, and for the effective coordination and articulation of response activities that can minimize economic loss, mitigate the impact on public well-being and loss of life.

> A national emergency telecommunication plan (NETP) sets out a strategy to enable and ensure communications availability during the disaster mitigation, preparedness, response and recovery phases, by promoting coordination across all levels of government, between public and private organizations, and within communities at risk.

Preparation and implementation of an NETP engages stakeholders to think through the life cycle of a potential disaster, it determines the required capabilities for emergency responses, and establishes a governance framework of roles and responsibilities. It also clarifies how to shape planning, envision and share desired outcomes, and it outlines effective ways to achieve and communicate expected results.

The NETP will reflect what diverse stakeholder communities need to focus on in order to address specific risks with available resources.

Additionally, for developing countries, the NETP will highlight major areas of risk. This not only provides support and justification for the funding of vital equipment and personnel in an emergency, but also promotes the need for day-to-day resources and procedures that keep national authorities prepared, especially to maintaining vital communications, the essential lifeline during emergencies.

This report assists national authorities and policymakers to develop a clear, flexible and user-friendly framework that guides countries on how to develop a strategic plan to support and enable the continued use of telecommunication and information and communication technology (ICT) networks and services in all four disaster management phases. It not only describes the main elements that an NETP should consider, but also highlights its potential benefits. It includes a step-by-step guide to the development of an NETP, it serves as a useful resource based on ITU recommendations and concepts, as well as expertise from other global bodies and organizations.

1.1 Scope and structure

This guide is intended primarily for national authorities responsible for the development and implementation of the NETP and is a useful resource for any person or organization generally involved in disaster risk management or in the administration of telecommunication/ICTs during emergencies. This includes governments, the private sector, non-governmental entities, humanitarian aid agencies, and private citizens.

This guide is designed to be flexible enough to be adapted to any kind of disaster that a country may face, it includes a full typology of disasters: climatological, hydrological, meteorological, geophysical and biological disasters (Annex B). Climatological, meteorological and hydrological disasters include both fast acting and more long-term disasters such as hurricanes and weather events as well as droughts and wildfires. These disasters can have local, regional, or global such as landslides, volcanic activity,

and earthquakes. The guide also addresses biological hazards, which includes insect infestations and epidemics of infectious disease. Beyond variations in geographic scope of the area impacted, disasters can have extended recovery periods that last long after the initial event. This guide addresses all phases of disaster preparedness and can be adapted to be used in response to all types of disaster.

Section 2 provides a step-by-step guide for developing an NETP. This section emphasizes the importance of including an overall risk assessment for the particular country in the NETP and describes the topics that should be included in the NETP. The section also sets out the phases of disaster management in order to incorporate them into the development of an NETP and presents a step-by-step process to draft the NETP.

Section 3 introduces the legal and regulatory framework, the administrative structure, processes and communication protocols that should exist in national governments for the implementation of the NETP, highlighting some relevant case studies, and considers the role the of institutions involved in disaster response.

Section 4 addresses issues related to regulation of communications; specifically, aspects regarding equipment imports, licensing of services, and the administration and planning of radio spectrum. It also discusses the potential to increase the ability of the regulator to address particular needs with greater flexibility.

Section 5 reviews how different networks and telecommunication/ICT services can be used in an emergency, and also reviews the literature on technical standards that exist for emergency management.

Section 6 outlines existing international cooperation and coordination mechanisms, as well as how they can be implemented by a given country.

Section 7 highlights the importance of continuous training, simulation drills and capacity building for all parties involved in the response to an emergency.

Section 8 describes the measures and activities that should be considered to help people with specific needs during emergencies, including children, the elderly, and persons with disabilities.

Annexes A, B, C, D, E, F and G provide supplementary information on topics addressed throughout the report and a reference section provides a list of relevant publications and ITU documents related to emergency telecommunication.

1.2 Recommendations

The following are the main recommendations the document offers to develop national emergency telecommunication plans:

- **Recommendation 1**: The NETP should take into consideration current capabilities, coordination challenges, planned resiliency requirements, with an understanding of the country's overall risk for telecommunication/ICT infrastructure and contingency planning, taking into account that hazards and vulnerabilities will vary widely between regions or even within countries. This overall risk analysis, developed jointly with telecommunication/ICT operators, should include geographic maps depicting the risk and telecommunication/ICT landscapes of the country.
- **Recommendation 2**: The NETP should include a description of the phases of disaster management based on the national disaster risk management plan adopted within the country and describe how telecommunication/ICT will be supported/enabled in each of these phases. The NETP should be governed by a set of principles that include, among others, addressing the country's potential hazards, participation from all stakeholders, both public and private, and the identification of all the telecommunication/ICT facilities that are required for different emergencies.

- **Recommendation 3**: The NETP should include clear administrative structures, processes and communication protocols essential to the satisfactory implementation of the plan, taking into account the specific needs, laws, regulations, institutions and other characteristics particular to a given country, including but not limited to, the national disaster risk management plan.
- **Recommendation 4**: Legislation and regulation regarding telecommunication/ICTs for disaster management should be in place or put in place and described in the NETP. Such legislation should provide high-level guidance on the development of the NETP, while still allowing regulatory flexibility during its construction and implementation.
  A description of the legislation, regulation, policies, and authorities related to telecommunication/ICTs for disaster management must be included in the NETP.
- **Recommendation 5**: The NETP should contain information on all existing telecommunication/ICT networks (public and private) available for use in a disaster event, a vulnerability and risk analysis of these telecommunication/ICT networks, and network contingency plans for when emergencies and disasters occur. This information should be periodically reviewed and updated.
- **Recommendation 6**: Multi-hazard early warning systems should be designed and deployed, linking all hazard-monitoring systems when possible to take advantage of economies of scale and enhance sustainability and efficiency through a multipurpose user-centric framework. An inventory of such systems, together with the processes used to activate them, should be included in the NETP and periodically reviewed and updated.
- **Recommendation 7**: The NETP should include a description of, and reference to, all international cooperation and coordination treaties and bilateral agreements that the country has signed regarding disaster management. In particular, countries are encouraged to take steps to ratify and implement the Tampere Convention and to take the necessary actions to put plans, policies, and procedures in place at national and local level, to ensure that the Convention and any other disaster management agreements relating to telecommunication/ICTs will be effective in a disaster situation. Such policies are necessary regardless of whether or not a country has ratified the Tampere Convention.
- **Recommendation 8**: The NETP should include a mechanism for enhancing training and capacity building for both the administrators leading emergency responses and the wider community using and providing telecommunication/ICTs in emergencies. This requires not only practice drills, training activities, tests and other exercises, but also the development of the curriculum for these activities and the evaluation and possible modification of any existing procedures and policies.
- **Recommendation 9**: The NETP should detail how to support continued availability of multiple forms of telecommunication/ICTs to provide messages and inform/alert impacted people, including those with specific needs, and marginalized communities. It is important to ensure that the NETP correctly describes, and appropriately responds to everyone's needs.
- **Recommendation 10**: Cybersecurity planning, defined to include prevention, detection, response, and recovery, should be included as a foundational requirement to ensure the confidentiality, integrity and availability of communications services to support emergency operations
- **Recommendation 11**: Annual exercises should be held and the NETP should be updated after every drill and operation to incorporate lessons learned and be fully reviewed at least every three to five years.

2. National emergency telecommunication plan: Step by step

This section first describes the need for a risk assessment, the topics to be included in the NETP, followed by a step-by-step process to draft the NETP.

2.1 Overall risk assessment

An NETP should be developed on the basis of a country's current capabilities, coordination challenges, and planned resiliency requirements, with an understanding of the overall risks for telecommunication/ICT infrastructure and contingency planning, considering that the hazards and vulnerabilities may vary widely between regions or even within the country (see Annex B).

While developing an NETP, each country will have to take into account such important elements as their geographical, topographical and political characteristics, among others, which can indicate the likely hazards and levels of vulnerability to a possible disaster. For example, a country in the Asia-Pacific could be exposed to flooding, hurricanes and earthquakes, as well as volcanic eruptions and tsunamis (see Annex C).

A risk assessment of the telecommunication/ICT sector can be achieved by mapping the different types of hazards and levels of vulnerability to a possible disaster against the telecommunication/ICT network infrastructure to see which areas of the network are vulnerable.

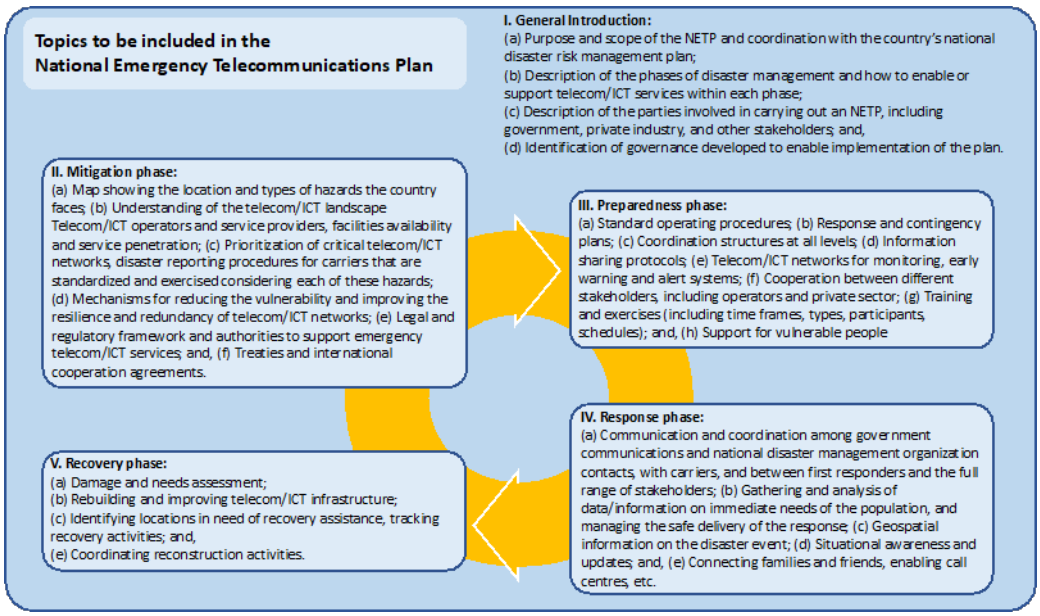
Recommendation 1

The NETP should take into consideration current capabilities, coordination challenges, planned resiliency requirements, with an understanding of the country's overall risk for telecommunication/ICT infrastructure and contingency planning, taking into account that the hazards and vulnerabilities will vary widely between regions or even within countries. This overall risk analysis, developed jointly with telecommunication/ICT operators, should include geographic maps depicting the risk and telecommunication/ICT landscapes of the country.

2.2 Topics to be included in the NETP

An NETP should be composed of at least five main sections. The first section is a general introduction to the NETP, and the following sections address the different phases of disaster management: mitigation, preparedness, response and recovery (see Table 1). Each section can be adapted to specific characteristics of each country. However, it is important to ensure that the topics described below are considered.

Figure 1: Topics to be included in a national emergency telecommunication plan



Source: ITU

Table 1: Topics to be included in a national emergency telecommunication plan

Topics	Description
General Introduction	(a) Purpose and scope of the NETP and coordination with the country's national disaster risk management plan. (b) Description of the phases of disaster management and how to enable or support telecommunication/ICT services within each phase. (c) Description of the parties involved in carrying out an NETP, including government, private industry, and other stakeholders. (d) Identification of governance developed to enable implementation of the plan.
Mitigation phase	(a) Map showing the location and types of hazards the country faces. (b) Understanding of the telecommunication/ICT landscape, operators and service providers, facilities availability and service penetration. (c) Prioritization of critical telecommunication/ICT networks, disaster reporting procedures for carriers that are standardized and exercised considering each of these hazards. (d) Mechanisms for reducing the vulnerability and improving the resilience and redundancy of telecommunication/ICT networks. (e) Legal and regulatory framework and authorities to support emergency telecommunication/ICT services. (f) Treaties and international cooperation agreements.

Topics	Description
Preparedness phase	(a) Standard operating procedures. (b) Response and contingency plans. (c) Coordination structures at all levels. (d) Information sharing protocols. (e) Telecommunication/ICT networks for monitoring, early warning and alert systems. (f) Cooperation between different stakeholders, including operators and private sector. (g) Training and exercises (including time frames, types, participants, schedules). (h) Support for vulnerable people.
Response phase	(a) Communication and coordination among government communications and national disaster management organization contacts, with carriers, and between first responders and the full range of stakeholders. (b) Gathering and analysis of data/information on immediate needs of the population and managing the safe delivery of the response. (c) Geospatial information on the disaster event. (d) Situational awareness and updates. (e) Enabling response, connecting families and friends, enabling call centres, etc.
Recovery phase	(a) Damage and needs assessment. (b) Rebuilding and improving telecommunication/ICT infrastructure. (c) Identifying locations in need of recovery assistance, tracking recovery activities. (d) Enabling and coordinating reconstruction activities.

2.3 Concepts and principles in a draft national plan

NETP principles

In order to develop a complete and effective plan for all sorts of risk management, an NETP should follow a conceptual guidance and a set of principles.

Figure 2: Principles of a national emergency telecommunication plan

Source: ITU

Table 2: Principles of a national emergency telecommunication plan

Principles	Description
Multi-hazard	• Adopt a strategy that addresses all potential hazards to which the nation is exposed. • During NETP implementation, decisions should be based upon the most accurate information available about all potential disaster types.
Multi-technology	• The NETP should make an evaluation of the telecommunication/ICT infrastructure to be used in all phases of disaster management. • Standard operating procedures should identify the appropriate types of telecommunication/ICT technologies required for each type of emergency. • The need for redundant communications networks should be planned for.
Multi-phase	• Ensure the NETP addresses the links between different phases of disaster management in different types of disasters.
Multi-stakeholder	• Increase awareness and obtain commitments from all relevant stakeholders to participate, contribute and agree on a strategy, enabling coordination with and communication among all partners. • The NETP should include training and drills prioritized, supported, and enabled, for all phases of disaster management and at all levels – individual, team, department and community. • During NETP implementation, decisions should be based upon accurate information/situational awareness. • Standard operating procedures should identify the appropriate types of communications/technologies that are required for each type of emergency.

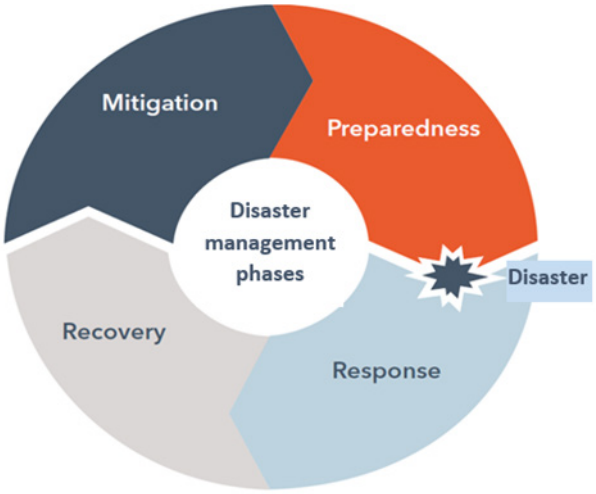
General introduction

Generally, the first section of the NETP describes how telecommunication/ICT services will be used to help prepare for and respond to disasters, and how communications as a national critical function will be prioritized and enabled in all phases of disaster management. In addition, the plan will discuss the application of these considerations across all levels of government, within communities, and between public and private organizations. This is done by defining policies, organizational structure and methods that inform the response to all phases of an emergency: disaster mitigation, preparedness, response and recovery.

The purpose and scope of the NETP should be in line with existing legislation and authorities on national disaster risk management plans and disaster relief. It is important that the NETP is incorporated into the overall national disaster risk management plan. The NETP must complement the national disaster risk management plan and include a description of the phases of disaster risk management as used in this plan (normally) mitigation, preparedness, response and recovery phases, see Figure 3),[1] and describe how telecommunication/ICT services can be used to support each of these phases (ITU, 2017c).

[1] The disaster risk management process adopted internationally by United Nations Office for Disaster Risk Reduction (UNDRR) consists of these four phases. See European Commission, United Nations Development Group and World Bank (2013).

Figure 3: Four phases of disaster management



Source: ITU

In this section, the NETP should include a description and inventory of the commercial, private and government telecommunication/ICT operators and networks that must be kept operational in a disaster event. It could also include the description of the availability and use of these services and map the infrastructure and services offered across the country, identifying those regions where there is a lack of telecommunication/ICT services.

Finally, in this section, the NETP should also reference any treaties or international cooperation agreements the country has signed related to telecommunication/ICT service cooperation for disaster relief, such as the Tampere Convention, or any partnerships with the private sector and the mechanisms that have been put in place to implement these. Since an NETP is dynamic, any new treaty, cooperation agreement or private partnership should be subsequently included in the NETP.

Mitigation phase

This phase includes any type of activity that seeks to prevent an emergency, reduce the likelihood of its occurrence, or limit the negative effects of unavoidable threats. The activities envisaged in the mitigation phase should be considered and implemented before and after the occurrence of emergency events.

In this phase, telecommunication/ICTs are used to facilitate the implementation of strategies, technologies and processes that can reduce death and property damage in potential disasters. Activities that should be carried out during disaster mitigation include establishing legal and regulatory frameworks that allow for flexibility in supporting and enabling the continued operation and restoration of telecommunication/ICTs, undertaking a risk analysis of critical communications infrastructure, taking steps to reduce the vulnerability of telecommunication networks, and improving their resilience (ITU, 2012). Telecommunication/ICTs are also used during this phase to coordinate the establishment and enhancement of infrastructure such as monitoring, early warning and alerting systems; establish procedures to address potential threats; and establish mechanisms to raise awareness and preparedness among citizens. Telecommunication/ICT, broadcasting and other mechanisms play a key role in the dissemination of information on how to mitigate the impacts of and prepare for a potential disaster.

Considering what types of disasters are unique to each country, the NETP should include a hazard profile of how and where the country is vulnerable. Existing geographic maps depicting the likely locations of different types of possible disaster may be useful to share with communications carriers. This is critical for the analysis of telecommunication/ICT infrastructure risks for both, the telecommunication/ICT industry and the government, and for drafting contingency plans, as well as for determining the type of warning systems needed. Risk analysis of critical telecommunication/ICT infrastructure is key to reducing the vulnerability and improving the resilience of telecommunication/ICT networks. This analysis must take into consideration the specific risk disaster map and hazard profile mentioned above, and the description and inventory of telecommunication/ICT networks, as well as national policies to enable ICT network operators to make networks more resilient.

Based on the infrastructure risk analysis, the NETP should include partnerships with telecommunication/ICT providers and private entities or establish regulations to incentivize the improvement of redundancy and resilience of telecommunication/ICT networks in specific locations that are at the highest risk in the event of a disaster. The NETP should also develop contingency plans to be executed if a disaster occurs.

The NETP should also describe the existing legal and regulatory framework and policies/procedures that support and enable telecommunication/ICT services in emergency situations. If no framework is in place, it will be necessary to draft a framework that supports the NETP and which provides authority for a government entity to, for example, request and support telecommunication/ICT infrastructure deployment from operators. As previously discussed, laws, regulations and policies, may determine coordination mechanisms, allocation of funds, communication channels, standard operating procedures (SOPs) and the identification of decision-makers at different agencies. If there is a legal and regulatory framework in place, it is necessary to see whether it includes all the necessary provisions to develop, exercise, implement and update the NETP on an ongoing basis.

Preparedness phase

This phase includes the planning and preparation necessary for responding to an emergency event. This includes the development of written plans and procedures, such as an NETP, to ensure that critical operations are maintained during and after the emergency.

A key objective of this phase is the development and improvement of coordination and communications mechanisms between those involved in disaster management and communications. This is achieved through continuous planning, coordination, training and mock exercises/drills, as well as activities designed to raise coordination and awareness among key stakeholders. The preparedness phase should also consider the creation of a set of procedures and measures to ensure communications are available to the diverse multi-stakeholder community when a disaster strikes in alternative and accessible formats. This includes the central government, local communities, state/provincial authorities, public safety officials, the private sector, relief organizations, hospitals, citizen-led groups and civil society organizations, the United Nations (UN) and foreign governments. Telecommunication/ICTs and other broadcasting services are key to facilitating the dissemination of warnings and alerts so the public is aware of actions they must take during an emergency.

Considering the above, a NETP should include detailed plans and procedures, as well as the protocols for coordination and communication of those involved in emergency management. Standard operating procedures (SOPs), *i.e.*, more detailed instructions on how to carry out the specific operational tasks or activities of emergency response, need to be included in this section of the NETP. This section should give key stakeholders a good idea of what should be expected and required of disaster response officials to ensure that telecommunications are available to a diverse multi-stakeholder community when a disaster strikes.

The NETP should include the functions, responsibilities and contact points, as well as contact details (e.g., e-mail and phone numbers –including for after hours), for each government agency and stakeholder related to telecommunication/ICT emergency services. This should be developed during the preparedness phase and regularly updated to account for reorganizations and changes in personnel.

Response and contingency plans should also be drafted and included in the NETP to establish arrangements in advance to set an environment to support the continued operation and restoration of communications, which enables timely, effective, and appropriate responses to disasters. Inputs to draft response and contingency plans should be based on the typology of disaster analysis and should identify the lack of telecommunication/ICT infrastructure in vulnerable regions.

Early warning and alerting systems should be deployed, tested and enhanced during the preparedness phase. In addition, an inventory of both new and existing monitoring early warning and alerting systems should also be included in the NETP. This should include, for each early warning and alerting system: information regarding the location, coverage and technology used by the system, as well as the type of hazards that specific early warning systems were developed for. This section should also address administrative aspects of early warning system (EWS), such as who is responsible for maintenance and operation of the system. Similar to telecommunication/ICT network infrastructure, the NETP should include an analysis of these early warning and alerting systems to address whether existing systems are fit for purpose: that is, whether the existing systems meet documented requirements and are scalable, flexible and accommodate new and emerging technologies, as well as appropriate for the type of disaster likely to occur, and whether the systems are well maintained and in good working order.

The NETP should also include guidelines for the telecommunication/ICT sector for all types of training, drills and mock exercises, starting with table-top exercises, then evolving in complexity to partial and full-scale drills and exercises. This improve teamwork, prepare teams to respond effectively to a real emergency, enhances knowledge of plans and procedures, and enable members to revise these as needed to improve their own performance and identify opportunities to improve system capabilities. These guidelines should be designed to implement lessons learned from these exercises during the preparedness phase: that is, before the actual emergency occurs.

How disaster response will offer support to vulnerable people should also be addressed in the preparedness phase.

Awareness and education of the population, including how to communicate most efficiently during a disaster and publicly available information on establishing personal/family emergency communications plans are key to increasing resilience, reducing risks and limiting fatalities and economic losses of the population. Telecommunication/ICTs and broadcasting services are important tools for carrying out this awareness and education. Regulations may be required to allow the government to use such networks to educate the public and increase awareness. It is recommended that the NETP incorporates these regulations, e.g., requiring broadcasters and mobile operators to support communication and messaging strategies to the affected population before and during emergency situations.

Daily usage of the emergency communications systems, familiarity with operational concepts and knowledge of how communications interconnect, to the extent possible, will also enable reliable and resilient communications and enhance capabilities so to be better prepared when needed for major incidents and disasters.

Response phase

In the response phase, the plans and procedures established in the preparedness phase are executed. This phase is carried out during the emergency and includes activities such as the evacuation of affected areas, the opening of shelters, search and rescue, or establishing telecommunications means to enable survivors to locate missing family members, among other activities.

During this phase, a set of actions and procedures are carried out by various entities to connect all actors in the disaster management ecosystem at the local, national and international levels. Therefore, a response plan should understand not only the channels of communication available, but also the types of information that need to be shared (ITU, 2017c). When a disaster strikes, coordination of relief operations is more efficient and effective if policies, well-drilled procedures and resilient infrastructure are available to all stakeholders.

Particularly, during the response phase, emergency telecommunication/ICT availability should be supported and coordinated among all stakeholders through the defined contact points. This is especially important considering that the need for interoperable and continuous communications capabilities for all responders is vital during the response phase of disasters. Therefore, during this phase, the designated coordinator or the lead government agency, working together with all relevant stakeholders and partners, should ensure that communications processes, partnerships and resources are effectively synchronized and utilized during response operations.

During this phase it is especially important that stakeholders help coordinate the provision of temporary satellite connectivity while networks are down and also help to restore damaged telecommunication/ICT infrastructure, because of the key role it plays for the government, private sector, non-governmental entities, humanitarian aid agencies and citizens in the aftermath of a disaster. While evaluating damage and attempting to re-establish networks in the aftermath of a disaster, communication must occur quickly and seamlessly between those who assess the damage and those who provide emergency communications services in order to establish priorities and direct the allocation of limited resources.

The NETP should incorporate procedures for obtaining information/situational awareness on the status of existing telecommunication/ICT capacities that should be supported to enable continued emergency disaster response. This should include, at a minimum, the following status items:

- Damaged infrastructure and services assessment (government and commercial/public networks).
- Development of a shared situational awareness and common operational picture for public-private coordination of impacted communications systems, services, and the mission impacts to disaster and emergency operations of each.
- Establishment of redundant emergency connectivity, based on priority setting.
- Maintenance and reestablishment of government networks, based on priority setting.
- Maintenance and reestablishment of commercial/public networks, based on priority setting.
- Regulatory or response actions needed to support continued operation and re-establishment of networks (access, credentialing, security, etc.).
- The need for potential flexible, expedited regulatory responses, to enable redundant means of communications in disasters.

Recovery phase

This phase occurs after the disaster and focuses on providing the help needed for the community to at least return to pre-emergency levels of safety and functionality, or to improve on pre-existing conditions. Activities during this phase include, among others, removal of debris, reconstruction of infrastructure, and restoration of public sector operations.

It is recommended to determine in advance, as much as possible, points of contact at relevant industry stakeholders for technical coordination implementing a standardized format and process with network operators for sharing network outage information. In addition, there should be backup (redundant) networks in place for government and first responder use in order to facilitate restoration efforts, such as dedicated government communications networks.

The rebuilding of more resilient telecommunication/ICT network infrastructure should also include potential redundant network deployments wherever possible to prepare for future disasters. Also, government and the private sector should take advantage of the opportunity to rebuild relevant telecommunication/ICT infrastructure, and where possible, to deploy technologies that are more resilient, efficient, and less expensive.

Finally, telecommunication/ICT networks and services should be used in this phase to help assess the damage and needs of the affected areas and population, identify locations in need of recovery assistance, track recovery activities and coordinate reconstruction activities. In addition, the identification of locations in need of recovery assistance and the amount and type required should be guided by a comprehensive assessment (Post-Disaster Needs Assessment) that estimates damages and losses and identifies the needs of the affected population. The development of this Post-Disaster Needs Assessment, among other elements, should consider logistic arrangements, including ICT needs, for example, or information management requirements.[2]

2.4 NETP drafting process

During the drafting of the NETP, it is important to include the views and opinions of all relevant government entities and private stakeholders that have responsibilities in the national disaster risk management plan. A preliminary list of these government entities and private stakeholders that could be included in workshops and interviews is shown below.

[2] For more detail, see European Commission, United Nations Development Group and World Bank (2013).

Table 3: List of government and private stakeholders to include in workshops and interviews

Entities	Description
Government	- Advisors to the Head of State (or Head of Government if possible). - If there is existing legislation/regulation relating to telecommunication/ICT, the people responsible for drafting such legislation/regulation. - National disaster management organizations (NDMOs) or whoever is responsible for coordinating the government response to disasters. - Meteorological bureau (in order to understand the main natural risks). - Ministry of foreign affairs (for aspects related to international cooperation and coordination). - Customs and Immigration offices. - Ministry responsible for telecommunication/ICT policy. - Telecommunication regulatory authority. - The governance structure responsible for spectrum policy/allocation (could be one of the above or an independent body). - First responders: police, firefighters, civil defence, etc.
Public telecommunication /ICT/media providers (voice, data–Internet, TV, radio, etc.)	- Mobile cellular service providers. - Fixed internet/telephony providers. - Satellite providers. - HF Radio. - Public Safety Radio Networks. - Public Safety Broadband networks. - High altitude platform providers for redundant communications. - Broadcasters (TV and radio). - Internet Service Providers. - Others present in the country.
Private networks	- Any government communications networks. - Amateur radio. - Private mobile radio providers. - Others (depends on what desk research reveals for a given country).
Civil society	These entities have first-hand information of the specific needs of the country for which the NETP is being developed and are critical to identifying the unique requirements of the country that must be addressed in the NETP.

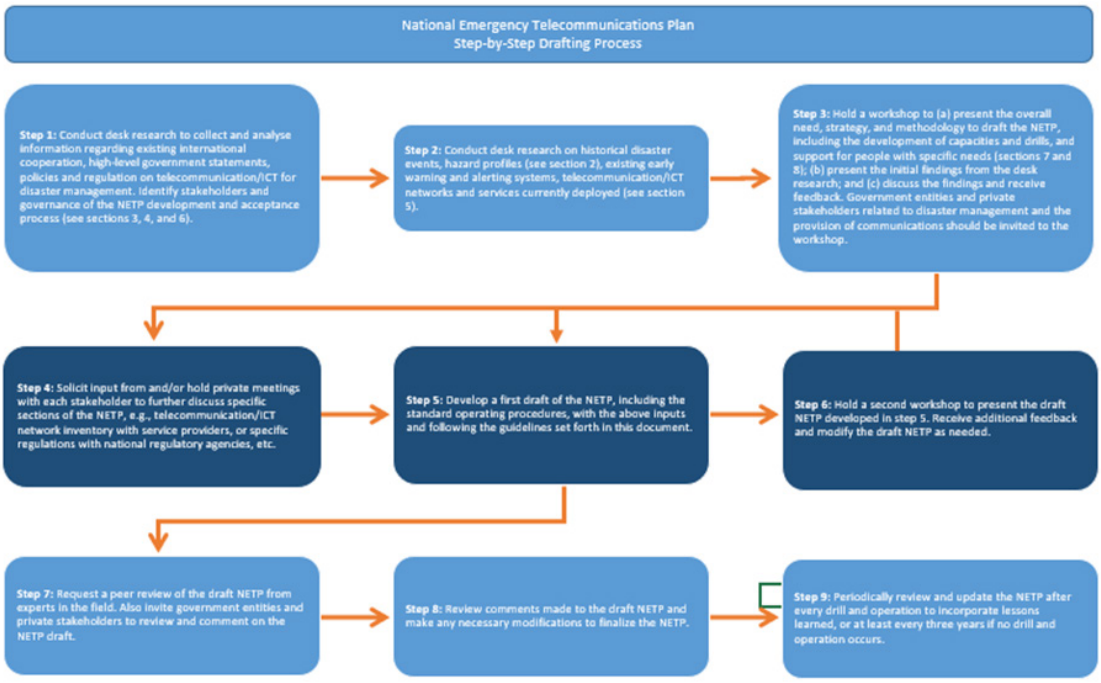
High-level steps

Based on the table above, the creation of an NETP should include the following high-level steps:

- **Step 1:** Conduct desk research to collect and analyse information regarding existing international cooperation, high-level government statements, policies and regulation on telecommunication/ICT for disaster management. Identify stakeholders and governance of the NETP development and acceptance process (see sections 3, 4, and 6).
- **Step 2:** Conduct desk research on historical disaster events, hazard profiles (see section 2), existing early warning and alerting systems, telecommunication/ICT networks and services currently deployed (see section 5).
- **Step 3:** Hold a workshop to (a) present the overall need, strategy, and methodology to draft the NETP, including the development of capacities and drills, and support for people with specific needs (sections 7 and 8); (b) present the initial findings from the desk research; and (c) discuss the findings and receive feedback. Government entities and private stakeholders related to disaster management and the provision of communications should be invited to the workshop.

- **Step 4:** Solicit input from and/or hold private meetings with each stakeholder to further discuss specific sections of the NETP, e.g., telecommunication/ICT network inventory with service providers, or specific regulations with national regulatory agencies, etc.
- **Step 5:** Develop a first draft of the NETP, including the standard operating procedures, with the above inputs and following the guidelines set forth in this document.
- **Step 6:** Hold a second workshop to present the draft NETP developed in step 5. Receive additional feedback and modify the draft NETP as needed.
- **Step 7:** Request a peer review of the draft NETP from experts in the field. Also invite government entities and private stakeholders to review and comment on the NETP draft.
- **Step 8:** Review comments made to the draft NETP and make any necessary modifications to finalize the NETP.
- **Step 9:** Periodically review and update the NETP after every drill and operation to incorporate lessons learned, or at least every three years if no drill and operation occurs.

Figure 4: National emergency telecommunication plan step-by-step drafting process



Source: Luxon

A checklist of topics to be addressed during the workshop and interviews is included in Annex A.

Recommendation 2

The NETP should include a description of the phases of disaster management based on the national disaster risk management plan adopted within the country and describe how telecommunication/ICTs will be supported/enabled in each of these phases. The NETP should be governed by a set of principles that include, among others, addressing the country's potential hazards, participation from all stakeholders, both public and private, and the identification of all the telecommunication/ICT facilities that are required for different emergencies.

3. National disaster management

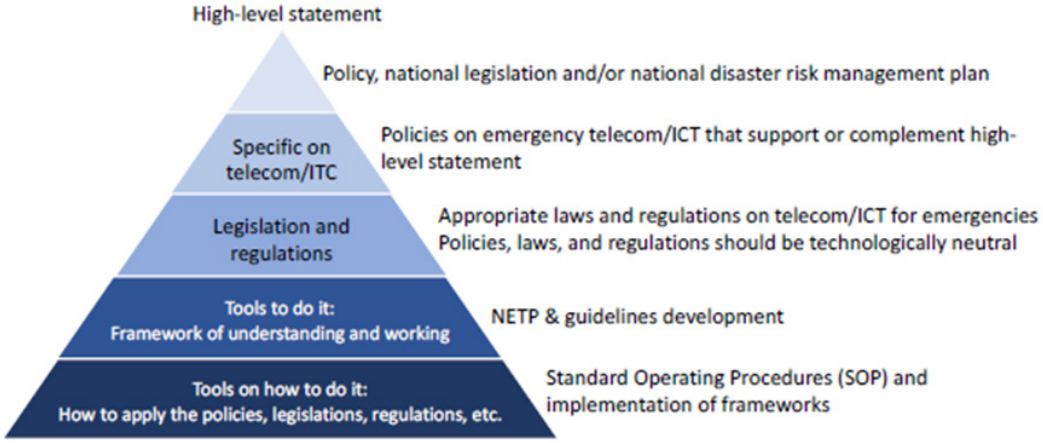
Clear administrative structures, processes and communication/coordination protocols are also essential to the satisfactory development, testing and implementation of the NETP. The establishment of clear policy and implementation frameworks is important not only for government agencies, but also for the organization and coordination of the different bodies involved, as described below.

The administrative structure and other aspects presented in this section can serve as a guide to be modified according to the specific needs, laws, regulations, institutions and other characteristics of a given country.

3.1 Legal and regulatory framework

Legislation and formal written rules are important to emergency management because they are the basis on which a country can define the responsibilities of those who play a role in emergency management (UNISDR, 2018). Laws and regulations can determine the framework for coordination mechanisms, communication channels and operating procedures, and identify the decision-makers at relevant agencies. Additionally, legislation and written rules can contribute to the sustainability of the disaster risk management process so that disaster management policies outlast individual government administrations, and secure, among other things, a budget independent from partisan politicking.

Figure 5: National emergency telecommunication development and implementation



Source: ITU

As Figure 5 shows, to develop an NETP, a country should start with the assumption that there is a high-level policy statement, national legislation and/or a national disaster risk management plan, that provides an institutional and inter-institutional framework for the actions of the government and civil society in the face of a threat or disaster. These national guidelines should be based on the premise that disaster risk management is the responsibility of all, with public, private and civil society participation in a multisectoral and interdisciplinary framework.[1] Likewise, planning should be endorsed at the highest levels of the government, which in turn must provide organizational and leadership support, as well as allocate resources and commit to deliver and maintain the desired outcomes.

The next step in the development and implementation of an NETP is to develop a specific set of policies on emergency communications that support or complement national legislation in the implementation of a comprehensive national approach:

- Policies should be designed to establish, develop or improve national interoperable telecommunication capabilities.

[1] UNDRR, available at www.unisdr.org (accessed 21 February 2019).

- Regulatory authorities and the government should issue appropriate rules and regulations, both technical and legal, corresponding to the implementation of national laws.
- Regulations, policies, and laws should be technologically neutral.
- National stakeholders, including telecommunication stakeholders, should establish a clear strategy and a robust process for the use of emergency communication services during national disasters based on these laws, policies, rules, and regulations.

While the national legislative framework and specific policies and regulations form the basis for an NETP, the plan should also define the methodologies and chain of command and coordination that will guide all stakeholders in the event of an emergency. An emergency telecommunication plan, specifically, cuts across multiple levels of response, supporting the continued availability of communications at all levels during an emergency, and describing how support of telecommunications will be managed in support of national disaster relief efforts to ensure an effective response to a disaster event.

Taking the above-mentioned rules as a starting point, the next step for a country should be to develop operating procedures, that is, more detailed instructions on how to carry out the specific operational tasks or activities of emergency response. These operating procedures should be designed to promote a standardized and uniform response during emergency response operations, and standardize use and application of interoperable emergency communications terminology, backup solutions and systems (United States Department of Homeland Security, 2014).

Standard operating procedures (SOPs) are critical, as they can help all levels of government understand how to manage their future emergency communication asset requirements and capabilities, and to enable the deployment of redundant mobile data services and applications. In this context, responding agencies should assess their needs for strategic, commercial, operational and tactical planning on a regular basis, and update them periodically.

Box 1: SAFECOM Writing Guide for Standard Operating Procedures[1]

The United States Department of Homeland Security, through their emergency communications advisory group SAFECOM,[2] developed a guide to help communities write their own customized SOPs. According to the guide, SOPs are "formal written guidelines or instructions for incident response, that typically have both operational and technical components, and enable emergency responders to act in a coordinated fashion across disciplines in the event of an emergency". Clear and effective SOPs are essential for any community to prepare and respond to an emergency.

Even though the SOPs should take into account the specific capability and/or resource that is the focus of the SOP, the reasons for which it is established and the unique characteristics of specific States or participating jurisdictions, the SAFECOM guide offers general direction on how SOPs should be developed, and includes clear recommendations on how they should be structured.

1 Based on United States Department of Homeland Security (N.D.).
2 Available at https://www.dhs.gov/safecom/resources (accessed 27 June 2019).

Box 1: SAFECOM Writing Guide for Standard Operating Procedures (continued)

According to SAFECOM, an SOP should incorporate the 11 sections described below:

(1) Introduction: Describes the recognized need for procedures and lists agencies that will share the procedures. It may also specify the capability/resource in which the procedures are being established and provide reasons why it is important to establish such procedures.

(2) Purpose: The purpose section of the SOP should clarify the principal objective of the capability or resource that is the subject of the SOP. It may also briefly describe the purpose of the SOP with respect to the capability or resource, and may include information as to authority, use, responsibility, etc.

(3) Scope: Lists the agencies and jurisdictions that will participate in the procedures and their relationship.

(4) Communications structure: A graphical depiction of the agencies involved in the communications structure should be incorporated in this section of the SOP. This can help map out the flow of information and help set the foundation for procedures.

(5) Channel patching and monitoring: This section is specific to shared channel capabilities. It describes how this can be achieved and the specifics of shared channels in each unique case. It can also serve to identify benefits and alternatives of the capability, as well as the specific procedures around aspects of use. This section may resolve questions such as whether a dedicated Ultra High Frequency (UHF) channel is patched to an 800 MHz network or not, for example, or who is responsible for monitoring the interoperability channel.

(6) Activation, transfer and discontinuation: This section describes rules of use for the interoperability channel, operation procedures for activation of the channel, authorities responsible for activation, process for transferring lead dispatch, process for establishing command and control, and procedures for discontinuation of use.

(7) Separation of the interoperability channel due to interference: This section is intended to outline the procedures to follow when there is interference with channel frequency. It should also include parties to be notified and actions to be taken in the event of interference.

(8) Communication alternatives: Several alternatives should be identified to ensure interoperable communications remain available among all agencies if the interoperability channel is not available. These alternatives include telephone conference bridges, computerized emergency notification systems, Internet/e-mail, or satellite phones, among others.

(9) Training requirements: This section is intended to state the objectives or the minimum requirements for satisfactorily completing training on the SOP. These objectives should accompany each training procedure.

(10) Testing requirements: Describes the procedures for testing the requirements of a capability or equipment.

(11) Responsibility: Finally, this section should state who or what body will ensure that all SOPs are followed.

3.2 Administrative structure and governance model

There are many diverse stakeholders involved in the different phases of disaster management. Therefore, if there is to be an effective preparation and response, a well-defined coordination structure should involve all relevant stakeholders. This includes local, national, and international stakeholders. Likewise, there should be a clear governance/coordination model that allows for planning, executing and revising activities to be carried out. These administrative structure and governance models should be flexible and adaptable to be able to fit each country's characteristics, in order to facilitate the implementation of the NETP.

Regarding administrative structure, the disaster management process takes place under the leadership (or request) of the national government, which defines the goals, roles, authorities, responsibilities and procedures for all relevant stakeholders at various levels acting in the face of a catastrophe. Indeed, based on the guidelines or protocols of action, efforts should be made to coordinate and define the responsibilities of sectoral institutions and their counterparts at all (e.g. regional, departmental, municipal and local) levels. In the elaboration of emergency and disaster care plans, distinctions can be made between the following: 1. Local, regional and national plans 2. Sectoral plans, and 3. Institutional plans.

The attribution of responsibilities in a disaster situation varies by country. In most cases, within the existing response structure of the country, a disaster operations coordinator is designated for each district, state, county or equivalent geographical division (ITU, 2001).

Box 2: The Colombia administrative structure and governance model[1]

In Colombia, Law 1523 of 2012 created the organizational structure of the National Disaster Risk Management System. This organizational structure comprises a set of public, private, and community organizations that, in accordance with established policies, norms and resources, aim to carry out the social process of risk management in the country.

Besides the national-level agencies, such as the National Council for Risk Management or the National Unit for Disaster Risk Management, which leads the risk management process at a national level under the mandate of the President of the Republic, Colombia's organizational structure is also composed of entities at the departmental and municipal levels. In the case of the departmental level, under the leadership of each governor, there is a Departmental Council for Risk Management, with its respective departmental committees for risk knowledge, reduction and disaster management. Meanwhile, at the municipal level, under the leadership of the mayors, there are also Municipal Councils for Risk Management and their respective Municipal Committees.

These departmental, district and municipal councils for risk management, in particular, are responsible for the coordination, advice, planning and monitoring that must guarantee the effectiveness and implementation of the risk management process in each area.

[1] Available at http://portal.gestiondelriesgo.gov.co/Paginas/Estructura.aspx (accessed 21 February 2019).

Moreover, *horizontal* cooperation between specialized services at each level of responsibility is as important as *vertical* (hierarchical) organization. With respect to disaster relief communications, it is vital to establish linkages between operation coordinators and telecommunication service providers within each level of the response hierarchy.[2]

[2] Ibid.

Also, this need for coordination between all national actors also applies to international humanitarian assistance. In that sense, it could be important to consider the following:

- Whether the government of the country where the disaster occurred should consider how and when it might request the assistance of or some other agency will foreign aid agencies, and how they will interface with them
- When requested by a country, United Nation emergency clusters[3] can play in the coordination of a response to a disaster by uniting agencies to work together[4]
- How organizing contact and coordination mechanisms and designating key contact points and leadership structures helps address preparedness in all phases, as well as enabling alert and early warning systems and procedures and facilitating drills and exercises
- National communications infrastructure, e.g., telecommunication operators, should be available, provide interoperability, and offer flexibility to any actor who relies on it before, during and after disasters.

Disaster risk management also requires the establishment of a clear governance model to support all phases of disaster management. This governance model should be flexible and adapted to fit the country's specific characteristics, and should align with national emergency management frameworks, plans and policies.

Effective governance requires accountability, transparency and meaningful participation by relevant stakeholders in all procedures and practices. A lack of accountability can create a possible leeway for corruption, increasing existing risk factors (UNDRR, 2018).

Engaged and effective governance is pivotal to operability, interoperability, and continuity of emergency communications. Robust governance can help establish and maintain coordination between stakeholders and can help address challenges in a unified way.[5]

To help further effective governance, SAFECOM and NCSWIC recently published a document that provides recommendations for disaster risk management, which proposes considering the following aspects for improving the effectiveness of governance[6]:

- Understanding the governance landscape: this is necessary to support a unified approach to and coordination of the multiple functions that encompass emergency communications. These functions include communications technology, and operational enablers; specifically, functions such as how governance bodies coordinate communication technologies (e.g., land mobile radio, broadband, 911, alerts, warnings, and notifications) and enabling factors (e.g., cybersecurity, public-private partnerships, non-governmental organizations with supporting roles, training, exercise, and evaluation programs).
- Building partnerships between response organizations at all levels of government, fostering interaction between different departments, agencies, and jurisdictions, as well as formalizing cooperation through written agreements: according to the document, forming relationships with other emergency management and public safety officials is one of the interoperability

---

3 The "cluster approach" was instituted in 2006 as part of the United Nations Humanitarian Reform process. It seeks to make humanitarian assistance more effective by introducing a system of sectoral coordination with designated lead organizations. Indeed, clusters are groups of humanitarian organizations, both UN and non-UN, in each of the main sectors of humanitarian action, e.g., water, health and logistics. They are designated by the Inter-Agency Standing Committee and have clear responsibilities for coordination. Sources: Available at www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach and www.who.int/hac/techguidance/tools/manuals/who_field_handbook/annex_7/en/ (both accessed 21 February 2019).

4 World Health Organization: www.who.int/hac/techguidance/tools/manuals/who_field_handbook/annex_7/en/ (accessed 21 February 2019).

5 SAFECOM and NCSWIC (2019), *Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials*.

6 Id.

coordinator's most important tools to break down barriers across levels of government and separate disciplines.

- Establishing a governance structure and formal decision-making processes through authorities, charters, by-laws, resolutions, and strategic plans: a strong governance framework supports a unified approach to emergency communications across multiple disciplines, jurisdictions, and organizational functions. For example, documentation of processes and decision-making structures could help evaluate existing communications capabilities, among other benefits. Written agreements between stakeholders also establish common goals and objectives and minimize risk for the communities served.
- Choosing a governance model that reflects the unique organization, needs, and potential partners of each emergency communications ecosystem: the authors suggest that since public safety equities can reside within multiple departments or agencies, establishing a governance structure provides opportunities for collaboration, resource sharing, and a unified approach to address challenges.
- Engaging in governance, including considerations for communications lifecycle planning, coordination with other governance groups, and integration of emerging technologies: by taking a wide view of the ecosystem, bodies essential for governance can ensure funding and sustainment policies are in place to maintain all communications technology functions. The document also suggests that partnerships between governance bodies to coordinate resources, share best practices, align policies, and adopt standards for neighbouring jurisdictions, can improve effectiveness.
- Enhancing governance by establishing mechanisms to measure outcomes and identifying solutions to common governance, legal, fiscal, and technological challenges: the authors suggest that proactively identifying capability gaps and implementing plans to achieve desired outcomes is key to overcoming challenges.

In conclusion, an active, transparent, multi-disciplinary, and multi-functional governance strategy for emergency risk management can help foster relationships, collaboration, and information sharing between all stakeholders. This, consequently, can help better balance fiscal, technological, and policy-driven public safety needs[7].

Finally, as part of putting in place an NETP, the government should consider what available telecommunication/ICT funding should be allocated for major disasters based on the risk profile of the country. These funds should be used to assist in all four phases of disaster risk management and should be specifically earmarked for emergency telecommunication/ICTs due to the crucial role they play in emergency response and coordination.

Box 3: The United Kingdom administrative structure and organizational model[1]

The National Emergency Plan for the Telecommunications Sector in the United Kingdom provides an overview of the response by the government and industry to any emergency situation that might impact on the telecommunication infrastructure of the United Kingdom. The document designates the Department for Business, Innovations and Skills as the lead government department for telecommunication policy, as well as establishing points of contact within the department and outlining the role for industry.

[1] United Kingdom, 2010.

[7] Id.

Box 3: The United Kingdom administrative structure and organizational model (continued)

The National Emergency Plan for the Telecommunications Sector in the United Kingdom provides an overview of the response by the government and industry to any emergency situation that might impact on the telecommunication infrastructure of the United Kingdom. The document designates the Department for Business, Innovations and Skills as the lead government department for telecommunication policy, as well as establishing points of contact within the department and outlining the role for industry.

In particular, according to the United Kingdom national emergency plan, the Department for Business, Innovations and Skills is responsible for leading the response to an emergency involving telecommunications, and shall serve as the key link for information flow between the telecommunications industry and the central government during an emergency. The role of industry, on the other hand, is to manage its internal response to any type of incident, while keeping the government informed of the possibility of occurrence of an emergency, among other responsibilities.

The United Kingdom plan establishes the information flow during an emergency as follows:

- Initial identification of any network disruption by a telecommunication operator.
- Activate National Emergency Alert for Telecommunications to disseminate information on network status, agree on industry actions for response and recovery, and estimate the time period required for restoration.
- Ensure that information regarding potential or actual emergencies with telecommunications implications is brought to the attention of the Department for Business, Innovations and Skills.
- Where relevant, ensure the safe operation of the telecommunication network during the emergency. This may require operators to isolate the systems that have faults so that they cannot cascade throughout the entire network.
- Manage the technical aspects of the emergency to ensure restoration of the network as soon as possible.

In order to promote efficient cooperation and flow of information, a non-disclosure agreement is provided in the United Kingdom plan, which protects any information shared from being circulated outside the emergency planning community. Furthermore, a memorandum of understanding allows the sharing of human and material resources among providers when required in an emergency.

Finally, the United Kingdom plan offers some guidelines regarding spectrum management issues so that, depending on the severity of the emergency, Ofcom, the United Kingdom communications regulator, could increase flexibility in licensing matters and the use of frequencies.

3.3 Public–private cooperation, coordination, communication plans

To develop and implement an effective NETP, it is helpful if all national agencies and stakeholders dealing with telecommunication/ICTs in emergencies provide support, ensuring the availability of telecommunication/ICTs for disaster management. This fosters awareness among all relevant stakeholders involved in emergency coordination both of the challenges they might face, and the measures necessary to address them.

Preparation for emergencies is more effective when plans are made jointly by public authorities and the private sector. However, many private sector companies may worry that sharing information publicly about the capacity or other characteristics of a network may be exploited by a competitor to give a commercial edge and they may exhibit reluctance when it comes to sharing information publicly related to network outages. Additionally, many companies have a continuity plan, which details logistics for the rapid restoration of services and the revalidation of data which may likewise be of interest to potential saboteurs. As a result, telecommunication/ICT organizations may wish to ensure that information provided is for use by the national government and only for national disaster preparedness and response purposes (ITU, 2001).

Consequently, it is important that state authorities leading emergency response coordinate closely with the private sector, keeping sharing situational awareness and developing trust. It is possible, for example, that network operators are willing to deliver sensitive information only to a select group of people that coordinate critical functions. Before undertaking an assessment on the vulnerability of telecommunications within disaster management, or any other type of risk assessment, it may be wise to establish a *confidentiality agreement*, a *memorandum of understanding* or a *non-disclosure agreement*, among other alternatives, in order to take into account the concerns of commercial entities involved in disaster response and thus obtain the required cooperation (United Kingdom, 2010).

These coordination and cooperation activities under the NETP can be led by the telecommunication ministry or regulatory authority in the country. In some cases, the government may need to establish a set of laws or regulations, and corresponding coordination mechanisms and procedures in order to ensure that the required cooperation from private stakeholders is available when needed.

Box 4: The Chile regulations on telecommunication networks for emergency management[1]

The Government of Chile approved regulations for the implementation, operation and maintenance of telecommunication networks for emergency management. These regulations established that the organizations involved in disaster management must designate an interlocutor to coordinate actions with the Secretary of Communications. This interlocutor, or Emergency Telecommunications Coordinator, must establish the procedures that will ensure that telecommunication networks for emergency management are operational when needed, as well as coordinate the restoration of communications, when necessary.

The regulations also established that the organizations involved in emergency management must ensure that the frequencies assigned to radio-frequency equipment for emergency response are periodically renewed, and that statistics are kept on the failures of emergency management telecommunication networks, along with a record of the preventive and corrective actions taken to prevent and correct such failures.

These organizations are also required to develop a plan to maintain redundancy of networks in case the emergency management telecommunication network becomes unavailable. Organizations must also keep a list of the contact information of each of the respective Emergency Telecommunications Coordinators and their alternative means of communication. Finally, the organizations involved must maintain an updated inventory of the telecommunication/ICT network infrastructure for emergency telecommunications and make periodic reports to the Secretary of Communications.

[1] Ministry of Transport and Telecommunications of Chile, Decree 125 of 2013 defines these organizations as "those entities and public services that, in accordance with current regulations, are related to any situation of catastrophe, emergency or public calamity, in order to avoid, detect or reduce the damages derived from these events".

3.4 Contingency plans

Contingency planning is an important part of disaster risk management and should be considered when developing an NETP. A contingency plan regarding telecommunications for disaster management implies establishing operational procedures to enable communications in specific areas. This scenario is associated with the specific or known risks in that specific location or that can suddenly appear, for example, a pandemic, flood, earthquake or any other hazard identified for that area. With this in mind, a contingency plan should include specific procedures such as the level of prior connectivity of the site, currently operational/available telecommunication/ICT facilities or pre-positioned equipment that could be deployed in the area, among others.

Unlike disaster response plans, which imply identifying, strengthening and organizing resources and capacities to reach a certain level of general preparedness for a timely and effective response, a contingency plan is intended to anticipate an event based on s*pecific or known risks*. Based on these risks, a contingency plan then establishes operational procedures (resources and capacity) for the response. Contingency planning implies making decisions in advance about the management of resources (including financial resources) and developing procedures for the expected use of the entire range of available technical and logistical responses, especially regarding communications.

For contingency plans to be relevant and useful, they must be an inclusive and collaborative effort. They should also be linked to the plans, systems or processes of both the government and other stakeholders involved at the national, regional and global levels (International Federation of Red Cross and Red Crescent Societies, 2012).

Box 5: Contingency plans for Covid-19[1]

Key to contingency planning is evaluating how normal rules of procedure can be modified in order to address specific and predictable risks and bottlenecks in the emergency response. During the ongoing Covid-19 pandemic, many countries are prioritizing the continued availability of services by modifying or expediting some of the following:

- **Frequency Allocation:** South Africa has expanded access to unused frequencies for mobile operators, including in TV white spaces. The United States of America has allowed temporary access to portions of the 600 MHz band to help mobile operators cope with increased demand.

- **Zero rating essential services:** In Mexico, the Federal Telecommunications Institute has required telecommunication operators to offer free access to reliable information on the pandemic disseminated through a designated list of official channels, including both on-line and over the phone.

- **Maintain access to services:** Many countries have taken action to ensure that subscribers maintain access to their telecommunication services as an indication of how essential these services are while many people are confined to their homes. These actions have varied by country but include suspension of late fees, expansion of access to Wi-Fi hot-spots, and temporarily stopping disconnections from service due to lack of payment.

- **Prioritize network maintenance:** In Colombia, the ICT Ministry designated telecommunication services as essential, allowing maintenance and repair crews to continue to travel to make essential repairs to network infrastructure in order to ensure continuity of service while lockdown measures are in effect.

- **Maximize network capacity:** In Colombia, the ICT Ministry requested that Internet platforms offer services in standard definition as opposed to more data intensive higher definitions that could overload already stressed networks.

- **Operator relief:** In recognition of the strain placed on operators during the emergency, governments have delayed payment dates for universal service fund contributions to allow operators greater financial flexibility. Other countries have relaxed regulations that required operators to maintain physical points of service for customer care, given that they run counter to broader objectives to maintain social distancing.

The common theme of these measures taken to respond to the Covid-19 pandemic is that they are designed to maintain availability and access to telecommunication services. This has required regulators and governments to assess how to overcome impediments to providing service that can help temporarily achieve the goals of expanded and reliable service during an emergency.

---

[1] ICASA (March 19th, 2020). ICASA engages with licensees to open their services to all South Africans as the country fights the covid-19 pandemic. Retrieved from: https://www.icasa.org.za/news/2020/icasa-engages-with-licensees-to-open-their-services-to-all-south-africans-as-the-country-fights-the-scourge-of-the-covid-19-pandemic Decree 464/2020 of the MINTIC, of March 23, by which measures are established in order to address the economic, social and ecological emergency situation determined by Decree 417 of 2020 (Diario Oficial, March 23, 2020).

3.5 Definition of roles and identification of contact points

Another essential issue to consider is that each of the institutions involved in disaster response should have a clearly defined role.

NETPs are designed to provide a guide for the management of telecommunications in disaster situations at a general level. As such, the leadership roles defined in the plans may vary according to the types of emergencies. For example, the Ministry of Health of a given country may have a leadership role when widespread outbreak of a particularly deadly disease occurs, but not for other types of disasters.

In that context, it is important that all stakeholders have their own standard operating procedures (SOPS) for the different types of emergencies and that these are aligned with the NETP and national coordinating mechanisms. It is recommended that the NETP is not only part of the national disaster or national emergency general plan, but also that policies and protocols are assigned to specific actors according to the agreed SOPs. This ensures that the NETP can be applied effectively in a variety of different emergency situations, including those unanticipated in the contingency planning, regardless of the particular agency taking the lead in response to a particular emergency.

In addition, administering an NETP framework also requires establishing contact points and identifying authorized decision makers within the different institutions involved in disaster management. This formalizes who will serve as focal points within the institutions, and thus improves communication, coordination and governance (accountability) within each level of the administrative structure.

The identification of contact points is also required for the development of sectoral SOPs and plans that define logistics, functions, responsibilities, resources and procedures in the event of a major national disaster.

Recommendation 3

The NETP should include clear administrative structures, processes and communication protocols essential to the satisfactory implementation of the plan, taking into account the specific needs, laws, regulations, institutions and other characteristics particular to a given country, including but not limited to the national disaster risk management plan.

4. Telecommunication/ICT legislation and regulation

Telecommunication/ICT legislation and regulation are critical for effective and efficient disaster management. Thus, a national law or set of laws describing high level, general and long-term telecommunication/ICT policies for disaster management needs to be in place. Regulatory authorities and government need to have the mandate to issue appropriate rules and regulations to implement the national law or set of laws. Such rules and regulations should describe in detail the responsibilities, protocols and strategies each stakeholder – including telecommunication/ICT operators, public and private organizations, government and the community – should implement to effectively and efficiently use, provide or facilitate emergency telecommunication/ICT services during national disasters. Considering that these rules and regulations also apply to telecommunication/ICT operators, it is important for the authorities to be flexible or open to understanding the industry challenges when developing them.

4.1. Legislation

Laws provide the legal authority for the regulatory agencies and the government to draft rules and regulations for disaster and emergency management plans, including the NETP. Such laws should provide general high-level guidance on the development of the NETP, while still allowing flexibility during its construction and implementation. These laws should give the government the mandate to, at a minimum, do the following:

- Outline the purpose and scope of the NETP: The NETP should support all four phases of disaster management across both the private and public sectors, with the purpose of maintaining communications ultimately to help save lives and reduce the negative impact of a disaster.
- Charge an existing or new government entity with drafting and periodically updating the NETP: This entity should be under the umbrella of the highest executive government level, e.g., office of the Head, NDMO, Head of State, telecommunication/ICT ministry or regulator. This entity should also be responsible for the drafting, implementation and updating of the NETP before, during and after the occurrence of an emergency or disaster.
- Define the functions and responsibilities of the entity, including defining how the entity will coordinate with different government institutions, e.g., ministries of foreign affairs, ICT and communications, customs, immigration, regulatory agencies and first responders, among others: The entity should also have authority to collaborate with the private sector, including telecommunication/ICT operators, private networks, amateur radio operators, etc.
- Define the governance structure of the entity.
- Provide the funding and human resources necessary for the entity to fulfil its responsibilities.
- Carry out the provisions based on specific national requirements and/or characteristics.

National legislation should empower government entities with legal tools to prepare for a disaster and also to manage requests from government institutions and the private sector, e.g., to develop (a) telecommunication/ICT national network infrastructure maps; (b) disaster risk and vulnerability maps; (c) specific telecommunication/ICT regulation to enable flexible authorities to address urgent needs such as temporary licensing, type approval, import/export of telecommunication/ICT equipment, and priority call routing; and (d) international cooperation agreements.

4.2. Regulation

Telecommunication/ICT regulation for disaster management should be in place and contacts and procedures known to all operators before a disaster occurs and should be aimed at maintaining and restoring communications to mitigate the negative impact that a disaster could cause. Rapid response in the wake of a disaster is critical. Consequently, regulations should streamline the process

to allow telecommunication/ICT services to be available as soon as possible, e.g., expedite or facilitate temporary licenses and type approvals, issue waivers as appropriate, reduce any barriers for import/export of equipment, allow for the free flow of experts who can assist in network restoration, grant temporary spectrum permits and suspend spectrum/license fees, among other actions. The NETP should promote and include telecommunication/ICT regulations, including the following:

- Telecommunication/ICT services licensing:

During a disaster, the telecommunication/ICT regulatory authority needs the authority and flexibility to grant on an expedited basis, telecommunication/ICT service licenses or approvals it deems necessary to support emergency telecommunication/ICT efforts. Therefore, flexible, exceptional expedited licensing procedures could be in place, free of charge, for use in emergency situations. These licenses should be temporary and valid only until such time as the government has determined that communications networks are restored to response areas and there is no further need for the temporary/redundant service being provided.

- Frequency allocation:

Frequency planning and allocation are critical for all four phases of disaster management: mitigation, preparedness, response and recovery. Frequencies should be available not only for narrowband and wideband systems, but also for rapidly growing broadband radio communication networks, both terrestrial and satellite systems.

Broadband radio communication networks would allow for bandwidth-intensive applications to be available to first responders, e.g., streaming real-time video, multimedia capabilities, high-resolution maps and images. Thus, governments could plan to make the necessary spectrum available on a national basis to allow for multiple types of applications and services, from narrowband voice services all the way up to broadband-intensive applications.

It is recommended that a combination of spectrum bands be allocated and available free of charge for emergency communications, allowing both terrestrial and satellite systems to be quickly deployed while also protecting incumbents from harmful interference in a crisis situation.

- Priority call routing:

During emergencies, networks fail to provide service for different reasons: e.g., power outages, infrastructure collapses and network congestion, which can delay or prevent critical communications between first responders. Regulations could be put in place to establish priority call routing on both mobile and fixed networks for people engaged in response and recovery activities during emergencies, as well as other entities and institutions involved in such activities.

- Network redundancy:

Network redundancy is a critical element of a robust network that will minimize telecommunication/ICT outages in the event of an emergency. Communications networks need to consider redundancy and resilience in their design to ensure that redundant capacity is available as needed. Regulators encourage and should ensure that telecommunication/ICT providers have networks with the adequate redundancy and multiple connectivity backhaul options.

- Type approval of telecommunication/ICT equipment:

During disaster response and recovery, type approval requirements for telecommunication/ICT critical equipment can be waived. Regulatory authorities can recognize foreign type approvals to expedite the process including by utilizing the guidelines of the ITU Telecommunication Standardization Sector (ITU-T).

- Importing telecommunication/ICT equipment:

Major delays during the importation of telecommunication/ICT critical equipment for disaster relief have a negative impact on the response time to a disaster, and even impact the likely loss of life if first responders are unable to use communications equipment to effectively reach areas with the greatest need. Delays can occur for several reasons, including a lack of priority given to communications when it is not considered an essential support function, a lack of coordination with customs (i.e., not informing customs that communications are a priority sector), imposing duties or tariffs on equipment provided for temporary use, restrictions based on local standards, extensive paperwork, disorganized processes, etc.

Rules could be in place to prioritize incoming communications equipment as being essential to response, and to expedite the importation process of critical telecommunication/ICT equipment for disaster response, e.g., exemptions from duties and tariffs, clear expedited processes and streamlined paperwork.[1] In addition, once the equipment needs to be returned to the place of origin, expedited processes should be in place to help streamline the return process.

Box 6: Regulations for telecommunication services during emergency situations in Peru [1]

In 2007, the Government of Peru established specific regulations regarding telecommunication services during emergency situations. Specifically, the Ministry of Transportation and Communications of Peru (MTC) approved the Communications System in Emergency Situations. This regulation included (a) a special communications network for emergency situations, (b) guidelines for disaster prevention, (c) guidelines for action during emergency situations and (d) guidelines for response in affected areas. In addition, MTC approved regulations for the promotion of amateur radio operators.

The main purpose of these regulations is to establish the obligations that apply to telecommunication providers during emergency situations, *i.e.*, offer telecommunication services to facilitate the coordination, prevention, security, relief and assistance activities to ensure the safeguarding of human life.

[1] Ministry of Transportation and Communications of Peru (2007).

[1] For more detail, see the Tampere Convention in section 6.3.

4.3. Ensuring regulatory flexibility

In order to reduce the negative impact of disasters, regulatory authorities could implement regulatory mechanisms that can be utilized in a disaster to increase the ability of the regulator to address particular needs with greater flexibility, such as the Special Temporary Authority, voluntary disaster reporting and public advisory efforts implemented by the Federal Communications Commission of the United States of America. Examples of these mechanisms are provided below:

- Regulatory flexibility: The Special Temporary Authority (STA), granted by the FCC, allows immediate or temporary operation of certain radio facilities during emergencies or other urgent conditions. These STAs are granted with a fixed expiration date, usually six months, or for the term necessary to cover the event. STAs, also, do not have grace periods and are valid only through their expiration date[2].
- Voluntary disaster reporting: The FCC Disaster Information Reporting System (DIRS) is a voluntary, efficient, web-based system that communications companies can use to report communications infrastructure status and situational awareness information during times of crisis. DIRS streamlines the reporting process and enables communications providers to share network status information with the Commission quickly and efficiently. The FCC determines whether to activate DIRS in conjunction with FEMA and announces to participating providers via public notice or email the area that will be covered by the activation and specifics about requested submissions.[3]
- Public advisory efforts: The Communications Security, Reliability and Interoperability Council (CSRIC) aims to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems. CSRIC members focus on a range of public safety and homeland security-related communications matters that include, for example, the reliability and security of communications systems and infrastructure, or emergency alerting.[4]

Recommendation 4

Legislation and regulation regarding telecommunication/ICTs for disaster management should be in place or put in place and described in the NETP. Such legislation should provide high-level guidance on the development of the NETP, while still allowing regulatory flexibility during its construction and implementation.

A description of the legislation, regulation, policies, and authorities related to telecommunication/ICTs for disaster management must be included in the NETP.

[2] https://www.fcc.gov/research-reports/guides/special-temporary-authority-licensing
[3] https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0
[4] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0

5. Telecommunication/ICTs for emergencies

This section describes the key information that should be collected and maintained by an emergency/disaster assistance office or other government entity, including, for example, a periodically updated database that generates maps with all existing telecommunication/ICT networks; a vulnerability and risk analysis of all telecommunication/ICT networks; and network contingency plans for when emergencies and disasters occur. In addition, this section addresses the elements that should be considered in EWS and includes a description of the standardized emergency format of CAP (Common Alerting Protocol). Finally, Annex D describes different public and private telecommunication/ICT services that should be considered in the development of an NETP.

As has been presented in previous sections, telecommunication/ICT facilities are essential in the management of operations before, during and after emergency and disaster events. The speed and effectiveness of emergency response depends on the availability of communications to enable the exchange of information in real time or as fast as practicable. In this sense, telecommunication/ICT services must be reliable and available when needed, including the rapid deployment of temporary capacity/services in priority areas in the wake of a disaster.

However, telecommunication/ICT services are only effective to the degree that responders receive the information that allows them to protect lives and livelihoods. In recent decades, a standardized emergency messaging format, the Common Alerting Protocol (CAP) (section 5.4), has been increasingly adopted. This simple but general format enables all-hazards alerting and warning over all kinds of media, thus increasing warning efficiency and effectiveness. The CAP message communicates the key facts of any hazard threat and the recommended actions. Implementation of CAP is considered an essential part of the NETP. This is implicit within Recommendation 3 in its provision that the NETP should include communication protocols essential to implementation.

5.1. Vulnerability and risk analysis of telecommunication/ICT networks

The government should maintain and update a map of risks and vulnerabilities of the telecommunication/ICT networks, taking into account the different types of disasters that may affect different regions of the country. It is essential to know the status of communications, including what communications carriers need to enable continued operation or restoration of networks and to take appropriate measures in advance to support the ability of carriers to exercise continuity plans to in the event of a disaster, e.g., increase redundancy of the network through satellite communications in additional to their terrestrial communication in critical facilities such as schools, utilities, police and fire stations.

In the event of an epidemic or pandemic, digital technologies and connectivity become critical enablers that facilitate business continuity, connect people, provide trusted information to the public, and prevent the spread of the epidemic. While ensuring network resilience for the provision of Internet access, network and service providers should also work to prevent cyberattacks and misinformation as well as issues related to data privacy and security.

Likewise, it is essential to be aware of existing telecommunication/ICT infrastructure and enact standardized disaster reporting in order to identify those regions in which there is no connectivity, and thus enable carriers to carry out contingency plans to provide communications services as soon as possible in the event of a disaster.

The government should encourage the coordination and collaboration with industry operators to maintain and update the map of risks and vulnerabilities.

Finally, the NETP should also encourage an adequate supply of pre-positioned telecommunication/ICTs and power equipment to be deployed during network outages. This equipment should provide redundant capacity as an emergency backup when networks are down. Stakeholders involved in disaster risk management could ensure that there is a continuity in the communication and information

flow by pre-positioning and safely warehousing the telecommunication/ICT equipment in places with low vulnerability to disasters.

5.2. Telecommunication/ICT database for emergencies

In order to carry out the analysis of risk and vulnerability of telecommunication services, as well as to plan before the disaster response, it is essential that the NETP provide for regular maintenance of an updated database of existing telecommunication/ICT networks. This database should include the capacity of the networks.

A telecommunication/ICT database for emergencies should include at a general level:

- telecommunication/ICT services available;
- terrestrial coverage;
- location of the specific infrastructure, e.g., towers, power stations, wired networks, etc.;
- pre-positioned telecommunication/ICT equipment location; and,
- vulnerability of the infrastructure to different types of disasters, considering, for example, high-, medium- or low-risk.

It is essential that this information be obtained jointly between the government and the different public and private telecommunication/ICT operators, as well as radio and TV broadcasting operators and amateur radio organizations mentioned in Annex D. Because this information may be confidential, it is important that agreements be established (or provisions included in the service license) to limit how the information obtained will be used, and ensure it is used exclusively for issues related to emergencies and disasters.

5.3. Early warning systems

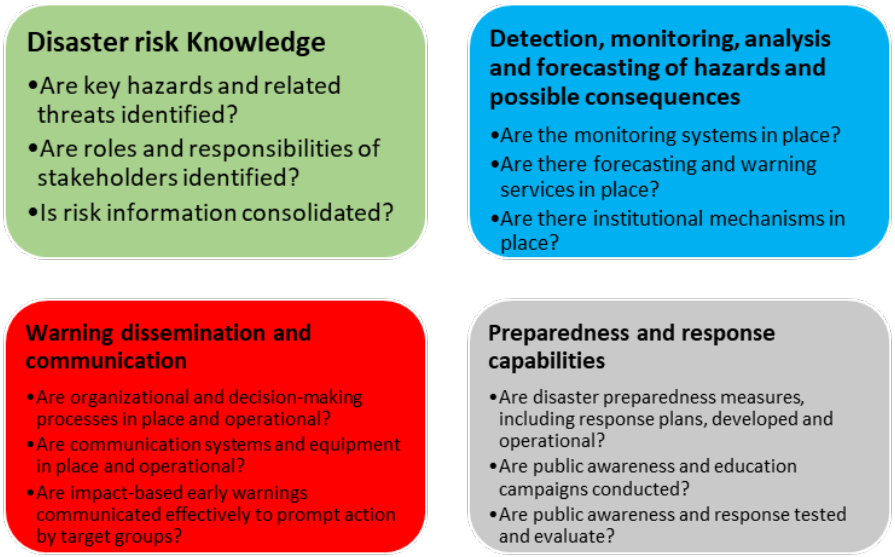
Telecommunication/ICT networks are also critical during the preparedness phase of disaster management through the deployment of early warning systems (EWS). Providing timely information to the population by means of telecommunication/ICT networks for monitoring, early warning and alerting is critical to reducing the impact of disasters and saving lives.

Early warning systems are define as "an integrated system of hazard monitoring, forecasting and prediction, disaster risk assessment, communication and preparedness activities, systems and processes that enables individuals, communities, governments, businesses and others to take timely action to reduce disaster risks in advance of hazardous events."[1] Warning systems include four elements of efficient, people-centred systems (WMO, 2018):

1. Disaster risk knowledge based on the systematic collection of data and disaster risk assessments.
2. Detection, monitoring, analysis and forecasting of the hazards and possible consequences.
3. Dissemination and communication, by an official source, of authoritative, timely, accurate and actionable warnings and associated information on likelihood and impact.
4. Preparedness at all levels to respond to the warnings received.

[1] United Nations (2016). *Report of the Open-ended Intergovernmental Expert Working Groupon Indicators and Terminology Related to Disaster Risk Reduction (OIEWG)* (A/71/644), adopted by the General Assembly on 2 February 2017 (A/RES/71/276)

Figure 6: Four elements of end-to-end, people-centred early warning systems



Source: WMO

EWS should, when possible, take advantage of economies of scale and enhance sustainability and efficiency through a multipurpose framework that considers multiple hazards and end-user needs (UNISDR, 2006b).

Meteorological satellites and Earth-exploration satellite services may be suited for identifying areas at risk; forecasting weather and predicting climate change; detecting and tracking earthquakes, tsunamis, hurricanes, etc.; and providing warnings/alerts about disasters, among other things. Even though warnings, alerts, and observations made on the ground, i.e., by terrestrial means, could be more precise than satellite observations, satellite observations are useful when terrestrial options do not exist or have been disabled by disasters.[2]

Resources such as satellite imagery can be helpful to map the location and condition (both pre- and post-disaster) of roads, bridges, medical facilities and other critical infrastructure, and provide precise information on this infrastructure so that first responders can make better decisions regarding relief efforts.[3] Thus, a comprehensive EWS strategy should use both terrestrial and satellite services to monitor possible disasters and provide accurate and timely warnings and alerts.

Early warning systems can be provided through the different telecommunication/ICT services described in Annex D. For example, broadcasting services can alert people of impending disasters, mobile systems can distribute notifications via mobile broadcast technology, specific apps developed by governments can provide warnings, etc. In addition, other types of warning systems, based on sirens or public address systems connected to sensors that trigger an alarm when a specific threshold is reached, can also be developed.

Radio and television broadcasting services are particularly useful when physical access to an area is difficult. Appropriate information and advice provided through broadcasting information can help people cope with the disaster until help arrives on-site. During disaster response, broadcasting services can provide information on how and where to access the help that is available, as well as other important information. However, it is important that the broadcaster use frequencies and modulation modes that match the receivers generally used by the population (ITU, 2017e).

[2] ITU (2010; 2017a). Recommendation ITU-R RS.1859 (ITU, 2010) provides guidelines on the use of satellite-provided remote sensing data in the event of natural disasters.

[3] See: http://www.missingmaps.org/

Box 7: The Butaleja district in Eastern Uganda: Flood early warning systems[1]

On 22 September 2014, ITU and the Uganda Communications Commission launched solar-powered flood early warning systems to warn residents of rising water levels of the Manafwa River. For many years before 2014, the Butaleja district in Eastern Uganda had been ravaged by flood waters from the river.

The warning system has three main components:

- a sensor placed in the river;
- a solar-powered siren adjacent to the river; and
- a solar-powered control centre at the district headquarters with backup computers to monitor the performance of the sensors and siren system.

Once the water levels reach a certain threshold on the sensor, it automatically activates the siren, alerting the communities using the local language and urging them to move to higher ground. The siren, which can be heard within a 10-mile radius, is followed by messages with additional information broadcast by the staff in the control centre.

Uganda flood early warning systems

Source: ITU

1 International Telecommunication Union, *Uganda: Harnessing the power of ICTs to promote disaster risk reduction* (https://www.itu.int/en/ITU-D/Pages/MakeADifference/How-we-make-a-difference-Uganda.aspx).

5.4. Common alerting protocol

Common Alerting Protocol (CAP) enables authorities to warn people of a disaster immediately, and up to global scale. People can receive CAP-originated warnings in many ways, such as through mobile and landline telephones, Internet (e-mail, Google, Facebook, Twitter, WhatsApp, smartphone apps, online advertising, Internet of Things (IoT) devices, in-home smart speakers, etc.), sirens (in-building or outdoor), broadcast radio and television, cable television, emergency radio, amateur radio, satellite direct broadcast, and digital signage networks (highway signs, billboards, automobile and rail traffic control), among others.

Figure 7: Common alerting protocol

Source: ITU

CAP-based alerting achieves this amazing diversity because the CAP standard defines a business form for alerting, communicating a few key facts of any emergency: What is it? Where is it? How soon is it? How bad is it? How sure are the experts? What should people do?

Alert messages in CAP format are machine-friendly as well as human-friendly. The CAP standard uses XML, the eXtensible Markup Language, to carry in one message machine-friendly data as well as human-friendly information. For example, in a CAP alert, the alerting area gets a text description and also a standard polygon or circle. Also, besides the capability of localizing warnings by drawing a polygon or circle, CAP allows alert messages to be broadcasted based on "FIPS" (Geo) codes. Those alerting area data allow all manner of telecommunication/ICT components to achieve targeted alerting to people in dangerous situations:

- Mobile phones get the CAP alerts through SMS or cell broadcast.
- Online users get the CAP alert automatically if they are using a Google online service.
- Sirens and in-home devices speak the CAP alert out loud.
- Broadcast radio and television automatically carry the CAP alert as crawl text or audio inserts.
- Some online users get the CAP alert as an overlay of online advertisements.
- Drivers see the CAP alert on digital billboards along the highway.
- Smartphones get CAP alerts through free apps such as the Red Cross Hazard App, which adds further information, such as where to find shelter and how to give first aid.

From a telecommunication/ICT technology perspective, CAP-originated messages can be disseminated via any kind of network, public or private. The typical architecture for CAP-originated messaging is fully scalable.

Box 8: Common alerting protocol[1]

In the United States of America, the Federal, state, local, tribal, and territorial alerting authorities can use the Integrated Public Alert and Warning System (IPAWS) and integrate local systems that use Common Alerting Protocol (CAP) standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface. The Integrated Public Alert and Warning System programme (IPAWS), established in the United States of America to "modernize and enhance alert and warning delivery to the American Public", uses Common Alerting Protocol (CAP) alerts to disseminate emergency information. According to the Federal Emergency Management Agency (FEMA), CAP "is a digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems".[2] In the United States of America, IPAWS uses a CAP standard that allows public alerts to be integrated and disseminated not only to conventional radio and TV, but also wireless devices, internet applications, and other future communications technologies. Further, IPAWS is a national infrastructure which provides the capability to allow state, local, territorial, and tribal officials to send public alerts and warnings. CAP Alert messages can include up to a 2-minute-long MP3 format voice clip, and, although video streaming is not supported, the alert authority can add the corresponding URL to an alert message.

Other countries besides the United States of America have deployed this technology in order to develop a more localized implementation. In Canada, for example, a working group composed of public alerting practitioners and government agencies developed a CAP Canadian Profile (CAP–CP) as a set of rules and standardized terms and values designed to address the needs of the Canadian public. CAP–CP includes services such as bilingualism, geocoding for Canada, and managed lists of locations and events, among others.[3]

China, on the other hand, has implemented CAP-enabled alerting for all hazards nationwide. The National Early Warning Release System gathers information from emergency command sectors and disseminates the information to the public and emergency management personnel throughout China (Christian, 2016).

In Australia, the CAP profile (CAP-AU) provides a formal national agreement on CAP, enabling all state and territory governments to improve the exchange and interoperability of hazard alert messages between systems. This system, according to the Australian Government Bureau of Meteorology, allows uniform text to appear as SMS text messages on the mobile phone handsets of people travelling into or through a warning area, and appear as text on electronic highway signs. The system also triggers the pagers of emergency service personnel and can activate warning sirens. In particular, persons with disabilities – including the deaf, vision impaired and people from non-English speaking backgrounds – can also benefit from this technology, which delivers consistent warnings and public-safety information through all available technology-based devices that are used to receive information.[4]

---

1 National Council on Disability (2014) and https://www.fema.gov/integrated-public-alert-warning-system.

2 Ibid.

3 Government of Canada, Canadian profile of the CAP-CP, available at www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/capcp/index-en.aspx (accessed 22 February 2019).

4 Australian Government Bureau of Meteorology, About CAP-AU-STD: The Australian Government Profile of the Common Alerting Protocol (CAP), available at www.bom.gov.au/metadata/CAP-AU/About.shtml (accessed 22 February 2019).

Box 8: Common alerting protocol (continued)

To overcome potential delays and ensure integrity of alert messages, it is important that a CAP based alert and warning system streamlines the process of gathering and disseminating alert messages to multiple channels. For example, after an alerting authority crafts a CAP alert message and sends it to FEMA IPAWS, the system will automatically authenticate, validate and seamlessly broadcast the alert message to desired dissemination pathways. This efficiency is the result of a great deal of interaction with alert originators during training and exercises with authorized IPAWS alerting authorities, supplemented by continuous coordination with industry and vendor communities.

Recommendation 5

The NETP should contain information on all existing telecommunication/ICT networks (public and private) available for use in a disaster event, a vulnerability and risk analysis of these telecommunication/ICT networks, and network contingency plans for when emergencies and disasters occur. This information should be periodically reviewed and updated.

Recommendation 6

Multi-hazard early warning systems should be designed and deployed, linking all hazard-monitoring systems when possible to take advantage of economies of scale and enhance sustainability and efficiency through a multipurpose user-centric framework. An inventory of such systems, together with the processes used to activate them, should be included in the NETP and periodically reviewed and updated.

6. International cooperation and coordination

International cooperation and coordination are important matters to consider when responding to an emergency, specially to ensure coherence in the management of risk of disasters. It is helpful to develop an understanding of existing treaties, conventions and other programmes that offer additional tools for use during and after emergency events. This is especially true in developing countries, where greater technical and humanitarian assistance may be required.

6.1 Emergency telecommunication cluster

Clusters are groups of humanitarian organizations whose aim is to "strengthen system-wide preparedness and technical capacity to respond to humanitarian emergencies, and provide clear leadership and accountability in the main areas of humanitarian response".[1] They also aim to enhance predictability, accountability and partnerships at the country level by improving prioritization and clearly defining the roles and responsibilities of humanitarian organizations.[2]

The Emergency Telecommunications Cluster (ETC) is led by the World Food Programme (WFP), and consists of a global network of organizations that work together to provide timely and effective inter-agency communications services in humanitarian emergencies.

In order to achieve the above, ETC relies on its network of members and partners, including the ITU, to carry out its critical work around the world. These members and partners also include UN agencies and programmes, NGOs, governments and other humanitarian organizations.[3]

6.2 International Telecommunication Union

This specialized UN agency, in cooperation with governments and the private sector, seeks, among other things, to coordinate the exploitation of telecommunication networks and services, and promote the global development of ICTs.[4]

Besides promoting the development of telecommunication/ICTs and spectrum management, all of which are useful and necessary in disaster management, ITU has also stipulated that the organization shall "promote the adoption of measures for ensuring the safety of life through the cooperation of telecommunication services" (ITU, 2006b), as well as prioritize the effective use of telecommunications during disaster and emergency response.[5]

In fulfilling this task, ITU produces a series of manuals on emergency telecommunications; develops emergency radiocommunication specifications applicable to all phases of a disaster (preparedness, mitigation, response and recovery); maintains a database of available frequencies for emergency radiocommunication services on land and space; and develops international standards on various technologies to cope with emergency situations, including the Emergency Telecommunications Service (ETS), the International Emergency Preferences Scheme (IEPS) and a Common Alerting Protocol (CAP).

---

1 Available at www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach (accessed 21 February 2019).

2 Ibid.

3 ETC members and Observers, available at www.etcluster.org/etc-members-and-observers (accessed 21 February 2019).

4 About International Telecommunication Union (ITU), available at www.itu.int/es/about/Pages/default.aspx (accessed 21 February 2019).

5 Through resolutions and recommendations adopted during recent World Telecommunication and Radiocommunication Conferences, as well as in ITU's plenipotentiary conferences, and through active participation in activities linked to the Tampere Convention.

6.3 Tampere Convention[6]

The Tampere Convention (see Annex E) is designed to facilitate the use of telecommunication resources for disaster mitigation and relief, by establishing a framework for international cooperation for states, non-governmental entities and intergovernmental organizations. It provides a legal framework for using telecommunications within the scope of international humanitarian assistance. This framework, when applied in conjunction with nationally developed procedures and bilateral and multilateral agreements, reduces regulatory barriers and gives protections to personnel providing telecommunication support, all the while respecting the national interests of the country receiving assistance.

In order to promote the use of telecommunication/ICTs by emergency teams, the Tampere Convention recognizes that it is necessary to abstain temporarily from the application of national legislation on imports, licensing and use of communications equipment. It also guarantees legal immunity to personnel who use emergency ICTs during catastrophes. The above is important considering that, in many countries, legislation continues to hinder, or even prohibit, (e.g., by applying restrictive laws to imports, organizational barriers or high costs) the arrival and timely installation of communications equipment in affected territories.

A country can express its consent to be bound by Tampere Convention by any of the following means:[1]

- by definitive signature;
- by signature subject to ratification, acceptance, or approval followed by deposit of an instrument of ratification, acceptance or approval;
- by deposit of an instrument of ratification.

[1] United Nations Treaty Collection, available at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXV-4&chapter=25&clang=_en (accessed 21 February 2019).

It is important to note the difference between the signature and the ratification:

Signing: include all the negotiations that precede the treaty. *By signing a treaty, a state expresses the intention to comply with the treaty. However, this expression of intent in itself is not binding. Sixty countries have signed the Convention.*

Ratification: approval of agreement by the state. *Once the treaty has been signed, each state will deal with it according to its own national procedures*. In the Netherlands, parliamentary approval is required. *After approval has been granted under a state's own internal procedures, it will notify the other parties that they consent to be bound by the treaty. This is called ratification. The treaty is now officially bind. Forty-nine countries have ratified the Convention.*

Nonetheless, ascension to an international treaty can require consultations or approvals of different legislative and executive bodies at the national level. It may also be necessary to adapt national laws and regulations to avoid conflict with articles of the treaty.

[6] Based on: www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf (accessed 21 February 2019).

It is important to consider that the accession and the adaptation of national laws and regulations are not sufficient to ensure that the Convention will be effective in a disaster situation. In particular, efficient implementation at the national level requires all of the different government agencies and national authorities involved in disaster management, including customs and excise officials at the border approving the importation of emergency equipment, to be aware of the treaty terms and to have put national procedures in place, and have a clear knowledge of the framework.

Finally, the Convention has binding force for those Member States that have expressed their consent to be bound by the Tampere Convention. However, bilateral or multilateral agreements between one or more countries that are not signatories can borrow provisions from the Convention or apply it in its entirety.

6.4 United Nations Office for the Coordination of Humanitarian Affairs

The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) is part of the United Nations secretariat and is responsible for bringing together humanitarian actors to ensure a coherent response to emergencies. Specifically, OCHA coordinates humanitarian action to ensure that people affected by a crisis receive the assistance and protection they need. OCHA also works to overcome obstacles that prevent humanitarian aid from reaching people affected by crises and provides leadership to mobilize assistance and resources on behalf of the humanitarian system.[7]

OCHA also acts as the Tampere Convention global operational coordinator[8] and, as such, it has a number of tasks aimed at improving coordination and information sharing with regard to telecommunication assistance. Among other responsibilities, the operational coordinator shall execute the responsibilities regarding general provisions, provision of telecommunication assistance, termination of assistance, and payment or reimbursement of costs or fees, as well as seek the cooperation of other appropriate United Nations agencies, particularly ITU, to assist it in fulfilling the objectives of the Convention.[9]

6.5 United Nations Office for Disaster Risk Reduction

The United Nations General Assembly appointed UNDRR as the secretariat of the International Strategy for Disaster Reduction. As such, this office has the mandate to guarantee the implementation of this strategy, and serve as the focal point in the United Nations system for coordination and synergies between United Nations disaster risk reduction activities, regional organizations and activities in the socio-economic and humanitarian fields.[10] UNDRR also supports the implementation, follow-up and review of the Sendai Framework for Disaster Risk Reduction 2015–2030.[11]

The UNDRR main duties include ensuring that the "reduction of risk of disasters" includes adapting to climate change; increasing investment for disaster risk reduction; building disaster-resilient cities, schools and hospitals; and strengthening the international system for "Disaster Risk Reduction", among others (United Nations, 2015a).

---

7 United Nations Office for the Coordination of Humanitarian Affairs, available at www.unocha.org/about-us/who-we-are (accessed 21 February 2019).

8 Tampere Convention, available at www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf (accessed 21 February 2019).

9 Ibid.

10 UNDRR, available at www.unisdr.org/who-we-are/mandate (accessed 21 February 2019).

11 Ibid. This framework is a voluntary, non-binding agreement that traces an approach to disaster risk reduction. See more at https://www.unisdr.org/we/coordinate/sendai-framework (accessed 5 august 2019).

Finally, UNDRR manages Prevention Web, a website with information on disaster risk management, and publishes reports regarding the management of emergencies on a regular basis, including a Global Assessment Report, along with other documents and statistics (ITU, 2013).

6.6 Bilateral agreements

Many of the existing international instruments for disaster response are in the form of bilateral treaties and agreements. These can be between countries, or even between the branches of international organizations and aid agencies in different countries. The scope of cooperation foreseen in these treaties varies widely but can include the donation of materials in response to a single emergency or formal technical assistance (e.g., training, assistance with relief personnel, and goods and equipment in place on the affected territory), among other things.

Regarding telecommunication/ICT, these kinds of agreements are very important in all phases of disaster management. Agreements between neighbouring countries, for example, can facilitate the deployment of telecommunication equipment in a timely manner after a disaster, or offer satellite solutions in cases where terrestrial communications services may have been damaged or networks are overwhelmed by increased traffic demands after an emergency occurs (Tampere Convention, 1998). Also, bilateral or multilateral agreements can be useful for countries where specific telecommunication/ICT equipment or services might not be available or are otherwise insufficient. These treaties can also be useful for sharing information and know-how regarding the use of telecommunication/ICT, capacity building or training on the use of equipment during the mitigation and preparedness phases, and deploying relief personnel or telecommunication/ICT experts during the response and recovery phases.

Recommendation 7

The NETP should include a description of, and reference to, all international cooperation and coordination treaties and bilateral agreements that the country has signed regarding disaster management. In particular, countries are encouraged to take steps to ratify and implement the Tampere Convention and to take the necessary actions to put plans, policies, and procedures in place at national and local level, to ensure that the Convention and any other disaster management agreements relating to telecommunication/ICTs will be effective in a disaster situation. Such policies are necessary regardless of whether or not a country has ratified the Tampere Convention.

7. Development of capacities and drills

Preparing for management of an emergency requires continuous training and capacity-building efforts for both those leading emergency responses and the wider community. The development of capacity requires not only practice drills, training activities, tests and other exercises, but also the development of the curriculum for these activities and the evaluation and possible modification of existing procedures and policies in light of limitations identified during capacity-building activities.

Capacity building is key to improving the speed, quality and effectiveness of emergency preparedness and response. Capabilities related to humanitarian needs (food, telecom/ICTs, medical supplies, shelter, etc.) must be developed with a focus on increasing the capacity of staff to respond to challenging scenarios, improving accountability and measurement of outcomes, and reducing risk of disasters where possible.

An effective NETP should include a practical strategy for enhancing the above-mentioned capacities and capabilities. Beyond the humanitarian needs identified above, enhancing capacity for emergency response must occur in all identified areas, such as institutional capacity, telecommunication/ICT network infrastructure and other areas identified throughout the planning process.

On capacity-building and skills development, focus should be on, but not limited to:

- identifying best practices in existing programmes and developing operating procedures and other guidance that respond to the needs of relevant stakeholders;
- enhancing emergency management programmes through better information sharing;
- identifying risk assessment and risk management methodologies;
- developing, documenting and maintaining information regarding national emergency management decision-makers;
- identifying critical infrastructure to better support emergency preparedness and response;
- conducting regional workshops, skills enhancement seminars and conferences; and
- developing and conducting various drills, including talk-through/walk-through exercises, and functional and full-scale simulations.

Additionally, training needs to encompass multiple subjects, from basic aspects of the use of telecommunication/ICT during emergencies to technical concepts. Training exercises should be held frequently, given the potential for high staff turnover in some of the organizations involved in disaster management. While in many routine operations it is common for new team members to learn their duties while doing the work (on-the-job training), this practice is not sufficient in the case of emergency telecommunications. Implementing periodic training exercises builds staff familiarity with additional responsibilities during an emergency event and allows them to familiarize themselves with some of the potential challenges that could arise (ITU, 2001).

Trainings must also be accompanied by practical activities, such as simulated emergency drills or tests held at all levels. These tests provide national training opportunities for individuals and groups, and highlight areas that require further improvement, be it additional training or upgrading of equipment.

Likewise, such training activities provide an opportunity to confirm the availability and reliability of emergency equipment that is not frequently used. Training exercises can help catch problems – for example, inadequate storage of equipment or deterioration of battery life – before responders must rely upon this equipment in a real emergency. These activities may also help reveal other issues, such as the loss of instruction manuals or auxiliary parts or lack of understanding of how to operate key equipment.

It is important to note that training exercises must be realistic enough to expose weaknesses in procedures or equipment, but at the same time must be simple enough so that inexperienced staff

can learn how an emergency response functions. After an exercise, time should be spent reviewing the deficiencies encountered and the mistakes made, so that the lessons learned can be noted and applied in a real emergency. Given that disaster response occurs in highly fluid situations, training exercises are one of the most dynamic, effective tools in the development of operational procedures and contingency planning.

In summary, effective training and exercise programmes can bolster emergency responders' proficiency with communications equipment, as well as improve their ability to execute policies, plans and procedures governing the use of communications (United States Department of Homeland Security, 2014).

Furthermore, training exercises and practical activities include terrestrial mobile radio systems to ensure that critical voice communications are available to emergency services during an emergency response. However, training exercises should also consider other communications technologies that might be integrated into response and recovery operations, including wireless broadband and satellite communications.

In addition, it is widely acknowledged that disaster response depends on teamwork. Therefore, it is important that training exercises include all potentially relevant stakeholders. Inclusive preparedness exercises increase the familiarity of all stakeholders with the specific roles of others involved in emergency response at the sectoral, organizational, and individual level. Within an organization, an understanding of the mandate and the working modalities of others involved in emergency operations is indispensable, in particular for those in charge of communications (ITU, 2001).

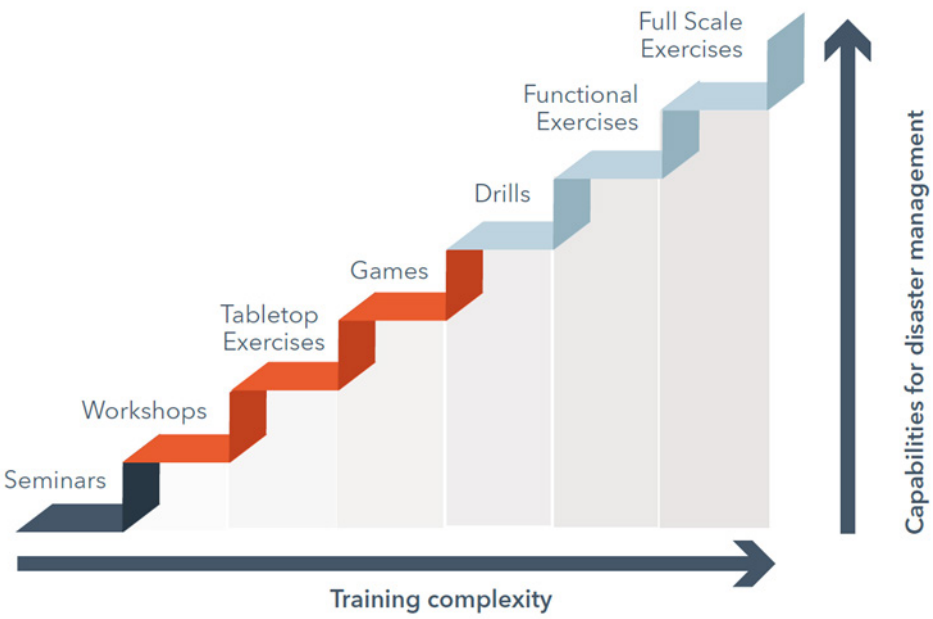
Finally, the NETP should establish some recommendations to use all available technologies and target gaps in emergency communications (United States Department of Homeland Security, 2014). These recommendations include:

- Develop training and exercise programmes that target gaps in emergency communications capabilities and use new technologies.
- Identify opportunities to integrate more private and public sector communications stakeholders into training and exercises.
- Use regional governance structures to develop and promote training and exercise opportunities.
- Leverage technologies, conferences and workshops to increase training and exercise opportunities.
- Promote awareness of and cross-training among local and national personnel responsible for communications through training and exercises.
- Develop and share best practices on processes to recognize trained communications personnel.
- Improve local territories ability to track and share trained communications personnel during response operations.
- Ensure that the capacity building process is continuous and account for the turnover in personnel.

Drills and simulations in practice

In the case of telecommunication drills and simulations (see Annex F), exercises should include as many different stakeholders as possible, to ensure a comprehensive response in an emergency situation. That is, these exercises should be designed to include participation from entities including the telecommunications regulator, ministry of telecommunications, national disaster management agency, meteorological and geophysics departments, telecommunication service providers (including the private sector and amateur radio groups), power utilities, humanitarian organizations (local and international) and communities.

Figure 8: Training ladder



Source: ITU

Appropriate planning is important for successful drills and simulations, and should consider the following factors:

- Start with a concept note that outlines the goal and expected outcomes of the exercise, including the required resources and the timeline. The concept note will introduce stakeholders to the exercise.
- Write the scenario: All exercises, from table-top exercises (TTX) to full-scale drills, require a scenario. The scenario is the script that sets the stage for the exercise. Ensure that the scenario is realistic and linked to the overall goals of the exercise.
- Create an evaluation plan: It will be the main element that makes the exercise a valuable learning experience.
- Conduct the exercise: Check that all equipment and other resources are in place. Brief the participants and then run the scenario.
- Monitor: Evaluate how participants respond to key events. Have the objectives and outcomes been met?

Finally, drills and simulations should end with an "after action" or debrief, in which the participants and facilitators of the exercise share their experiences, challenges faced, and provide feedback. This is the most important part of an exercise. The debrief should set the course of action for areas that need improvement or adjustment, as well as identify the areas of strength.

Box 9: NetHope[1]

ETC partner NetHope conducted a preparedness training and field exercise in Panama in July 2018. It was designed to offer a real-life experience configuring wireless networks in the field, as well as to develop capacities such as team building, leadership abilities, agility and working together toward a shared purpose.

The training hosted more than a dozen expert trainers, several observers, a documentary filmmaker, and more than 50 participants from 9 of the 56 NetHope member organizations (SOS Children's Villages, CARE, Catholic Relief Services, Christian Aid, International Federation of the Red Cross and Red Crescent Societies, Medical Teams International, Mercy Corps, Plan International, and Save the Children) and employees from tech partners Facebook, Microsoft, Google and Amazon Web Services. It consisted of two parts: (a) classroom training on both technical matters and the mental and physical challenges of being deployed in disaster situations; and (b) an in-field re-enactment of a disaster situation that was held on the grounds of Ciudad del Saber, a former United States of America military base located alongside the Panama Canal.

All the trainers were experienced emergency responders from NetHope, Cisco, Ericsson Response, Red 52, and Save the Children, each having deployed many times to a variety of disasters, including earthquakes and hurricanes. The planning of the exercise included identifying, shipping and storing thousands of kilograms of communications and power equipment from many different locations, arranging travel, housing and meal logistics for more than 75 participants and support staff, finding and securing locations for the exercise to take place, and designing the presentations and simulation scenario, among other activities.

[1] NetHope (2018), ***Planning a disaster: detail and expertise required for disaster preparation training***.

Box 10: Earthquake drills[1]

In 2015, local governments in Japan implemented earthquake drills as part of the 2015 Comprehensive Disaster Management Drill Framework. Among other exercises, the framework developed a drill to test crisis management systems, including initial response, information gathering and transmission. In this drill, exercises were conducted to gather and transmit information on how disaster management-related organizations use communications networks such as the Central Disaster Prevention Radio Network and satellite-based mobile phones. Also, the framework included a drill to secure and manage lifelines, such as electricity, gas, water and communications lifelines, among others. The drills were also an opportunity to inspect relevant equipment and ensure it was being used appropriately.

[1] World Bank (2016), ***Learning from disaster simulation drills in Japan.***

Box 11: gear.UP[1]

gear.UP is a large-scale inter-agency operational exercise and functional training event designed to further advance emergency response capabilities of the global ICT and logistics humanitarian community.

ETC and the UN Logistics Cluster work together to integrate aspects of the full-scale field simulation exercise (OpEx Bravo) and the Logistics Response Team Training (LRT). The combined exercise – called gear.UP – allows each cluster to practice various emergency response functions, providing opportunities to support each other as they would in a real emergency.

This exercise involves an intensive seven-day field simulation held annually and led by WFP as global leader of ETC and the UN Logistics Cluster. In the field, the exercise tests, among other things, IT and telecommunications, including satellite connectivity, networking and drone operations, as well as other skills, such as coordination and information management. Apart from the above-mentioned agencies, the exercise is developed in conjunction with FITTEST[2] Training Services, the German Federal Agency for Technical Relief (THW), and the Government of Luxembourg. OpEx Bravo and LRT is held near Stuttgart, Germany at the THW Training Centre. Participants from UN agencies, Stand-by Partners and NGOs are also invited to attend.

---

1 Emergency Telecommunications Cluster, OpEx Bravo and LRT (gear.UP), available at www.etcluster.org/training/opex-bravo-lrt (accessed 22 February 2019).

2 The Fast Information Technology and Telecommunications Emergency and Support Team (FITTEST), is a team of qualified instructors from WFP, each with extensive experience in both emergency and development settings. (See www1.wfp.org/FITTEST and www.etcluster.org/content/wfp-fittest-training-services, both accessed 22 February 2019.)

Recommendation 8

The NETP should include a mechanism for enhancing training and capacity building for both the administrators leading emergency responses and the wider community using and providing telecommunication/ICTs in emergencies. This requires not only practice drills, training activities, tests and other exercises, but also the development of the curriculum for these activities and the evaluation and possible modification of any existing procedures and policies.

8. Support for people with specific needs

Disasters are especially difficult for vulnerable people, such as persons with disabilities, children, the elderly, migrant workers, the unemployed, people with lack of connectivity skills and those displaced from their homes due to previous disasters. It is important to ensure that disaster management plans reflect and respond to their needs. The following is a series of recommendations for inclusive disaster planning (ITU, 2017a; 2017c):

- Consult with members of vulnerable populations directly and facilitate their involvement at all stages of the disaster management process.
- Ensure that accessibility and usability of telecommunication/ICTs are considered during any project on telecommunication/ICT-based disaster management processes or telecommunication/ICT-based development projects.
- Use multiple strategies and mechanisms to promote accessible telecommunication/ICT, including legislation, policy, regulation, license requirements, codes of conduct and monetary or other incentives.
- Build the capacity of vulnerable populations to use telecommunication/ICTs in disaster situations through programmes to raise awareness, trainings and skills development programmes.
- Use multiple modes of communication to provide information before, during and after disasters, including vulnerable groups:
    - accessible websites and mobile apps designed as per current Web Content Accessibility Guidelines (WCAG);
    - radio and television public service announcements (including methods to increase accessibility, such as audio, text, captions and sign language interpretation);
    - announcements and advice sent through SMS; multimedia messaging service; mass e-mails to citizens from government authorities, aid and relief agencies, and others;
    - accessible electronic fact sheets, handbooks and manuals;
    - multimedia, including presentations, webinars, webcasts and videos, including on popular sites such as YouTube;
    - dedicated social media such as Facebook pages and Twitter accounts created by governments and disaster response organizations;
    - citizen-focused working groups and discussion forums.
- Be aware of the potential for misuse of personal data of vulnerable populations in disaster situations, and develop ethical norms and standards for data sharing.
- Provide information packs, guides and manuals; conduct public awareness campaigns in multiple accessible formats in different languages; and provide sensitized resource persons to impart the contents of these packs to persons with disabilities and other vulnerable groups.
- Develop, promote and distribute mainstream and assistive technologies that can be used during emergencies and disasters, and provide the necessary training to persons who use them.
- Develop frameworks to facilitate inter-agency collaboration and conduct drills and trust-building initiatives.
- Specify accessible telecommunication/ICT infrastructure as part of procurement guidelines wherever applicable.
- Ensure that all services, facilities and infrastructure developed after a disaster are accessible and inclusive.
- Provide information in multiple formats and through multiple modes about ongoing recovery efforts and how to get help or access resources.

- Review disaster response efforts to assess any challenges for vulnerable groups, discuss lessons learned, and undertake efforts to fix any issues in telecom/ICT-based disaster management services.

The use of several different types of telecommunication/ICTs can be vital for supporting all people including people with specific needs such as those with disabilities during emergencies, considering the different difficulties that could arise according to the type of disability. We are all possible users of different types of telecommunication/ICTs (anyone with a permanent or temporary disability could be in need of a specific type of technology based on the specific need of that specific moment). Therefore, it is important to ensure that technologies provide several alternatives to communicate and ensure that every person can be able to communicate based on his/her abilities. For example, blind people cannot see, but they can hear; paralyzed people can hear and see, but they cannot run, or a blind person or a person that just had cataract surgery will not see but will be able to hear; a person with a mobility impairment or a person with a broken leg will not be able to run, etc. The deaf or hard of hearing can see, but they cannot hear alarms, EWSs, radio reports, or any other kind of alert or auditory information. Consequently, the strategies for preparing and responding to emergencies should include all available telecommunication/ICTs and take into account all possible needs that every person might have.

Telecommunication/ICTs can be a key tool in disaster response and management operations, providing the possibility to use multiple modes and channels to reach all people, without discrimination of age, gender, ability or location. Apart from traditional forms of telecommunication/ICT (TV and radio), the world of telecommunication/ICTs includes different mechanisms that can facilitate communication to people with disabilities: landlines, mobile audio, text/SMS messages and Internet-based services and resources such as websites, video, instant messaging over the Internet, voice services on Internet protocol, web conferencing, social networks that allow instant communication and exchange of photos/videos and satellite communications.

However, the content for disaster preparedness and planning materials may be inaccessible for all people unless these are created and delivered in multiple formats through multiple media. For example, public television advertisements, online videos and exclusively audio-based web transmissions will be inaccessible to deaf people unless they are accompanied by subtitles or interpretation of sign language. Other examples of the incorporation of multiple forms of telecommunication/ICTs are presented in Annex G.

Box 12: Wireless Emergency Alerts[1]

Wireless Emergency Alerts (WEA) is an alert protocol in the United States of America with the purpose of broadcasting emergency alerts to mobile devices. This system enables geographically targeted alerts and warnings in the form of text-like messages that are broadcast only from cell towers in the specific area where the emergency occurred. Also, these messages sent by WEA include a distinctive attention signal and vibration that is noticeable for people with hearing impairments or vision-related disabilities.

Since its launch in 2012, the WEA system has been used more than 40 000 times to warn the public about dangerous weather, missing children and other critical situations, all through alerts on compatible mobile phones and other mobile devices. It has also enabled government officials to target emergency alerts to specific geographic areas – Lower Manhattan, for example.[2]

1 National Council on Disability (2014).
2 United States Federal Communications Commission. Wireless Emergency Alerts Consumer Guide. Available at www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea (accessed 22 February 2019).

Box 13: PLUSVoice[1]

PLUSVoice Co. is a Japanese company that offers a free remote video relay service in areas hit by the earthquake and tsunami of 2011 in Japan for people who are deaf or have a hearing impairment. This technology uses sign language interpreters to give relevant information to people in Iwate, Miyagi and Fukushima shortly after a disaster occurs. The free videos can be accessed via smartphones.

PLUSVoice began its remote interpreting service in 2002 through videophones placed in government offices and shops, so that people with hearing problems could communicate with officials and shop clerks. The company expanded the service the following year, aiming directly at individuals who used videophones, e-mail and faxes (Japan Times, 2012). The company introduced the free remote video relay service in 2012, taking advantage of the increased usage of smartphones.

This service is very useful in countries such as Japan where, according to a 2006 estimate by the Health, Labour and Welfare Ministry, the number of people with hearing or speech disabilities in Japan is nearly 360 000.

1 Qureshi (2012), ***Accessible ICT tools and services in disaster and emergency preparation.***

Box 14: Get Ready Get Through[1]

The Government of New Zealand created a website called Get Ready Get Through,[2] which includes information in accessible formats, such as MP3 files, e-text, DAISY talking books, audio CDs and cassettes, and Braille. The website contents are also available in multiple languages.

In particular, the website provides information on types of disasters, such as earthquakes, storms, floods, tsunamis, volcanoes and others; how to create and practice a household emergency plan; and how to assemble and maintain an emergency survival kit. It also gives recommendations regarding getaway kits in case people are forced to evacuate at short notice.[3]

1 Qureshi (2012).
2 Get Ready Get Through, available at www.getthru.govt.nz/ (accessed 22 February 2019).
3 Ibid.

Recommendation 9

The NETP should detail how to support continued availability of multiple forms of telecommunication/ICTs to provide messages and inform/alert all impacted people, including those with specific needs, and marginalized communities. It is important to ensure that the NETP correctly describes, and appropriately responds to everyone's needs.

Annex A: Emergency communications checklist[1]

I. Preparedness

a) Administration and responsibility setting

Establishment and clarification of roles and responsibilities within a government and with stakeholders is one of the most basic – but critical – parts of developing a disaster communications management plan. Points of contact should be identified within the various agencies, and decision-making authority and responsibilities in key areas should be clarified. In cases where there may be overlapping expertise or responsibility within an agency, or across multiple agencies, governments should work in advance to clearly determine leads and lines of responsibility to save time and improve the overall response when disaster strikes.

Government roles and responsibilities

- ☐ What government agency/ministry is responsible for disaster management and response overall in the country?
- ☐ What other ministries are involved/should be involved in disaster preparedness and response? What are their respective roles or mandates? What is the role of the communications regulator and ministry? Is the communications ministry or regulator a participant in the activities of the national disaster management authority?
- ☐ What authorities (legislation or mandates) enable each ministry/agency to respond to certain aspects of disaster response that will help guide identification of leads and roles and responsibilities?
- ☐ Who leads on particular aspects of response in each of those agencies in the event of a disaster? Does that lead vary depending on the type of disaster? How is disaster response coordinated within a ministry and organization? Who are the backup points of contact in case the disaster impacts the lead person? What authority/decision-making ability does each point of contact have and in what area/subject matter?
- ☐ How does the lead disaster management ministry coordinate with other relevant ministries across government? How frequently does the core contact group coordinate, meet or conduct drills/exercises between disasters? Who maintains the point of contact list, and how often is it updated? Does it contain all possible contacts both for home and work?
- ☐ How is telecommunication/ICTs prioritized or addressed within the country's disaster management framework?
- ☐ How is disaster response management responsibility or authority managed between central government and local or provincial/state governments?

b) External coordination

Disaster response involves many actors/stakeholders, such as the central government, local communities, state/provincial authorities, public safety officials, the private sector, relief and technology organizations, hospitals, citizen groups and civil society organizations, the UN, and foreign governments. In order to support an effective and coordinated response, a disaster communications plan should incorporate these external actors (stakeholders), and they should be actively involved in preparedness activities.

[1] ITU (2017c).

I. Preparedness

- ☐ Ensure coordination processes, define partnerships and establish points of contact with external organizations. These may include:
  - private telecommunication entities (carriers and equipment);
  - other ministries;
  - local and state/provincial government agencies;
  - NGO relief and response organizations, hospitals;
  - United Nations/ ITU;
  - foreign governments/military;
  - volunteer technical communities;
  - Amateur radio;
  - Citizen and community groups, civil society organizations.
- ☐ Who are the actors in your country that have been involved in or could improve/enable disaster response? Which foreign/international actors could support the response? How are citizens and local communities involved in disaster response planning? How are citizens informed about disaster response plans?
- ☐ Who are the points of contact in each organization, and how will the government engage/exchange information with those organizations before, during and after a disaster? What types of information or situational awareness can be shared by these stakeholders? What types of information or situational awareness can be provided to these stakeholders to facilitate a response?
- ☐ How will you coordinate with these actors/stakeholders when developing a disaster response plan? How will you coordinate with these actors in any preparedness activities? How frequent will those communications or interactions be? What is your stakeholder engagement strategy or plan? Does your government have any requirements or legislation governing stakeholder engagement, public outreach or advisory committees?
- ☐ Do external international actors require credentialing to enter the affected areas or visas to enter into the country when a disaster occurs? Have expedited processes been established in advance for both the entry of experts and communications equipment in times of disaster?
- ☐ How are persons with disabilities and specific needs included in preparedness activities? How are these specific needs taken into account in planning?

c) Training and exercises

Once roles and responsibilities are defined, exercises are the best way to prepare teams to respond effectively to an emergency. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events with further training and education.

I. Preparedness

Exercises are a great method to:

- evaluate a preparedness programme;
- identify planning and procedural deficiencies;
- test or validate recently changed procedures or plans;
- clarify roles and responsibilities;
- obtain participant feedback and recommendations for programme improvement;
- measure improvement compared with performance objectives;
- improve coordination between internal and external teams, organizations and entities;
- validate training and education;
- increase awareness and understanding of hazards and the potential impacts of hazards;
- assess the capabilities of existing resources and identify needed resources.[2]

Some considerations are provided below:

- ☐ Is training or certification mandatory for officials designated to support a response effort? Consideration should be given to what type of training or certification may be needed for each type of personnel, and how regularly it should take place.
- ☐ Do exercises include both internal stakeholders and external, non-governmental partners? Consideration should be given to how regularly exercises take place among various stakeholders. Are drills conducted to ensure that the public is aware of disaster response plans and can recognize and react to a warning (for example, how to respond if an early warning alarm is triggered)?
- ☐ Are telecommunication/ICT exercises conducted separately and/or as part of more comprehensive national disaster exercises? How do national disaster exercises incorporate the role and priority of addressing telecom/ICTs?
- ☐ Which communications exercises are held (e.g., Early warning system testing, or regional/national outage responses and restoration)?
- ☐ Are exercises tailored to the types of disasters known to your country, *i.e.*, extreme weather, flood, earthquake, wildfires, humanitarian responses or cyberattack?
- ☐ Which agencies or ministries oversee and participate in communications-related exercises or drills? What are their roles? What is the role of local communities or governments?
- ☐ How are stakeholders – such as communications operators and suppliers, and technology-focused organizations/associations – engaged in disaster response or disaster communications exercises? Are they part of the exercise planning process?
- ☐ Are outage reporting requirements of carriers exercised? Do carriers follow a uniform reporting process, and know which contacts to report outages to and how?
- ☐ Is online training available for stakeholders prior to exercises?
- ☐ How is feedback collected after an exercise to help improve procedures or performance? Which stakeholders would you request feedback from? Is an "after action" report done, and is it circulated to participants?

[2] United States Department of Homeland Security, available at www.ready.gov/business/testing/exercises (accessed 23 February 2019).

I. Preparedness

d) Infrastructure and technology

Telecom/ICTs are a critical tool facilitating disaster early warning, relief and response. One objective of a disaster communications plan is to help ensure the continuity or restoration of communications in the event of a disaster. Below are some considerations related to infrastructure and technology when developing and implementing a disaster communications management plan during the preparedness phase.

- Technology inventory or assessment: A wide range of technologies and services can and should be used to support disaster communications response. When developing a plan, it is helpful to take stock of the technologies used by stakeholders (government, responders, citizens) to communicate on a daily basis, and which are often used in times of emergency. Such technologies could include emergency dispatch services; amateur radio; first responder systems, including radio and public safety broadband; television and radio broadcasting; terrestrial mobile networks; wireline voice networks; broadband networks; satellite networks; and social media.
- Redundancy and resiliency planning: Ensuring operational continuity and preparing for continuity and restoration of primary communications channels to minimize outages.
- Power: Available and pre-positioned power sources (for infrastructure and individuals). What backup power resources are available for operators, governments, responders and citizens, and how are these resources prioritized for restorations? Are processes in place to expedite or facilitate fuel delivery for communications network generators? Are there guidelines in place for critical facilities to have backup power supplies?
- Identification and training of key public and private personnel: Regular training should take place for those personnel who will need to use and maintain/test emergency communications equipment. Local communities and local staff should also be considered for training in the use and maintenance of such equipment.
- Identifying critical sites/priority sites for restoration: What mechanisms are in place to prioritize critical sites for restoration efforts? How are these priority sites communicated to, and discussed with operators?
- Establish situational awareness and reporting mechanisms (public/private sector cooperation), such as a communications-focused advisory committee: How is information about business continuity plans exchanged with government officials?
- Spectrum and frequency planning: Licensing/authorizations, including expedited frequency and type approvals, emergency spectrum management and authorization, expedited licensing approvals and possible temporary/emergency authorities: Has there been an assessment of any regulatory or policy barriers to entry or operation of needed equipment for disaster relief or restoration of networks?
- Priority and expedited customs procedures for approved/authorized incoming communications equipment.
- Consideration of emergency and network resilience/redundancy needs/requirements in national telecommunication development plans (e.g., broadband or infrastructure development plans).

I. Preparedness

- Human factors: Preparedness plans should take into account that many personnel or their families may be directly impacted by a disaster and will be operating under stressful circumstances.
- "Harmonized" outage reporting: To increase situational awareness and more rapidly identify needed resources for telecommunication/ICT restorations or to provide appropriate information to the public, authorities can identify terminology and a common format for reporting of outages to ensure a common understanding of status and requirements.
- Use of "Big Data" analytics to support disaster prediction and forecasting or projecting possible impact or risk, and to support decision-making and allocation of resources: What data sets are available for government or public use to aid in disaster response and risk reduction planning? What policies are in place to ensure that data can be shared by operators with responders in a way that protects individual privacy, while enabling response? What collaboration or public–private partnerships could support improved use of data in support of disaster preparedness?
- Establishing emergency alerting systems:

    1) Mechanisms and technologies (broadcast, mobile, machine-to-machine/sensor networks; remote sensing technologies; Big Data; integration of delivery mechanisms, social media): What technologies and applications are best suited for the environment, geography, type of disasters and method of communication needed by citizens? Are multiple platforms used to ensure information gets to those affected? How should existing alert systems adapt to new technologies while also ensuring the broadest delivery of alerts? How to incorporate social media platforms?
    2) Alert content (language, CAP, accessibility considerations): Which officials are empowered to authorize the sending of an alert? What consideration is given to ensuring citizens are informed, while avoiding "alert fatigue"? What information is placed in an alert and what standard is used to avoid confusion?
    3) Enabling policies: Expectations of carriers or broadcasters, policies and procedures for preparing, approving and disseminating messaging.
    4) Regular/ongoing national and regional alerting exercises and system testing: Who is involved in testing? How often will tests take place?
    5) Public education: Working with local communities and civil society to recognize early warnings and act on them.
    6) How do alerts and early warning systems take account of those most vulnerable to disasters, such as persons with disabilities, including radio and television announcements or alerts, and information distributed through SMS, e-mails, etc.

I.	Preparedness

- ☐ Accessibility considerations:
  1) How are members of vulnerable populations consulted regarding their needs? How are capacities of vulnerable populations developed, for example, through awareness-raising programmes or trainings? Are information materials, including websites or apps, accessible?
  2) Are accessibility and usability of ICTs considered in projects? What strategies and mechanisms are used to promote accessible ICTs, including legislation, policy, regulations, license requirements, codes of conduct, and monetary or other incentives?
  3) Are information materials provided targeting vulnerable populations? Are public awareness campaigns conducted in multiple accessible formats in different languages, along with sensitized resource persons to impart the contents of these packs to persons with disabilities and other vulnerable groups?
  4) Following a disaster, are disaster response efforts reviewed to assess challenges for vulnerable groups, discuss lessons learned, and undertake efforts to fix any issues in ICT-based disaster management services?

II. Response, relief and restoration

a) Communications channels and information sharing

Telecom/ICTs are tools to support exchange of critical information between those affected by a disaster, including citizens and those participating in response, relief and restoration activities. While operational continuity or ongoing availability of the underlying technologies is important when developing a response plan, it is also important to understand the channels of communication and types of information that need to be shared. Flexibility is important, as needs quickly evolve during a disaster.

- ☐ What Information is being communicated? What types of information are needed (and could be provided) by certain parties? (These types of information include network outage status; safety and location of family members or key personnel; meteorological and seismic information; the location of shelters; damage and infrastructure assessments (including status of roads or transportation systems to allow for movement of supplies or personnel); rules and regulations associated with emergency equipment approvals and operation; response coordination, including what supplies or personnel are needed to support relief and restoration efforts; and who is able to provide support).
- ☐ Who is communicating? What are the channels of communication? Who has priority to communicate?
  - Intragovernmental communications.
  - Government to UN or NGOs that provide relief and response.
  - Interactions between Government and UN/NGO responders and private sector (telecommunication/ICT providers).
  - Government to public, UN/NGOs to public.
  - Public to government/UN/NGO community.
  - Private sector to public.
  - Private sector to private sector.
  - Citizen to citizen.
- ☐ Are backup or diverse/redundant means of communication in place in case of outages? Has consideration been given to whether a disaster may render a planned communication tool unusable and what redundant means of communication might be used? (For example, if the expectation is to communicate via conference call, how will accommodation be made if the phone networks are down?) Are portable communication units available to establish temporary connectivity?
- ☐ Ensuring accuracy of data/verifying information: Consideration should be given to how to verify and report/disseminate information before acting upon it to ensure the most efficient use of resources and improve coordination and decision-making.
- ☐ Understanding cultural norms and behaviours: Different cultural groups may communicate in different ways, or trust information from different types of sources. Consideration should be given to linguistic and cultural behaviours and how they affect communication.
- ☐ Social media: How can social media be used as a tool for collecting data and sharing information for two-way communications? How do relief and response authorities respond to requests for help received via social media? What partnerships can be established to best use social media tools? How do citizens use social media for information gathering and exchange during a disaster, as compared with other tools?
- ☐ Establishing mechanisms for communicating across and with diverse groups; sharing information/situational awareness/reporting.

II. Response, relief and restoration

b) Infrastructure and technology

In evaluation of damage and re-establishment of networks, communication must happen rapidly between those assessing the damage, determining priority of restoration efforts and directing assistance, and those providing emergency communications services. Determinations should be made in advance, whenever possible, about points of contact for functions such as technical coordination and sharing of network outage information. In addition, there should be backup (redundant) networks in place for government and first responder use in order to facilitate restoration efforts, such as dedicated government communications networks.

Evaluation of damage/ICT assessment

- ☐ What is the role of the communications ministry/regulator regarding reporting damage or outages to public or commercial telecommunication networks and enabling continuity and restoration, and how is that role defined (through a license, etc.)?
- ☐ Who will be the designated ministry/regulator or point of contact to collect, analyse and react to/report/release information regarding damage to networks? What information and analysis from operators should be obtained and utilized? How will these information needs be communicated in advance to operators?
- ☐ For those networks that are commercial or public, are there reporting requirements already in place that would establish a process, format and timeline for submitting evaluations? If not, can government set up a coordinating mechanism by which to establish expectations and receive information?
- ☐ Will initial damage assessments be connected to award disaster recovery funding?
- ☐ For government networks, which inter-agency coordination and information-sharing processes will need to be established? Will public or private networks be more suitable/reliable for this purpose?
- ☐ Are there policies in place that consider communications network status, needs, conditions and requests, and that enable the maintenance and restoration of the following communications capabilities? What process is followed to determine the priority of each restoration?
    - Local agency land mobile radio systems.
    - Emergency dispatch services.
    - Status of terrestrial systems/public mobile systems.
    - Broadcast radio/TV stations.
    - Amateur radio services.
    - In-country VSAT provider availability.
    - Pre-positioned emergency MSS equipment.
    - Internet services.

II. Response, relief and restoration

Establishment of emergency connectivity

- ☐ Which emergency telecommunication partners will be contacted in the event of a disaster? What information will be provided to them, and how will they be contacted?
- ☐ How will offers of assistance from foreign governments, humanitarian organizations or the private sector be received and processed?
- ☐ Who are the points of contact to authorize incoming equipment or allocate requested frequencies? Is there a mechanism to ensure timely coordination with local operators to avoid interference?
- ☐ Which emergency ICT resources will be pre-positioned and at which priority locations, and by whom? Who has authorization to activate or distribute? How will these pre-positioned resources be maintained and tested? What consideration is given to fuel supplies for power generators and restoration of telecommunication networks?
- ☐ Ensure coordination between telecommunication teams and the central disaster management institutions to meet needs: Consider which networks and communications technologies are most used by first responders (e.g., land mobile radio vs. mobile data services), or by the public to reach emergency services, and could therefore be prioritized for immediate restoration or additional maintenance support. How can government agencies facilitate private sector restoration of networks?
- ☐ Where will emergency connectivity be first established? Consider whether there are previously determined disaster recovery sites that will require immediate connectivity, or whether connectivity will be required for mobile disaster recovery centres.

II. Response, relief and restoration

Maintenance and re-establishment of networks

- ☐ Is there a source of expert advice and assistance for government agencies with respect to restoring government networks and telecommunication infrastructures? In cases where government uses private networks, will restoration be carried out by government or private sector technicians? Consider whether there are commercial networks in place to use as backup for closed government networks in the event of disruption. Does government have mechanisms or emergency procedures in place to facilitate customs clearance or import of equipment needed for restoration of critical networks, or to facilitate entry of any external expert personnel needed to restore and rebuild networks?
- ☐ Is there a process in place to routinely test networks designed for emergency communication?
- ☐ Are commercial or public network operators encouraged to have a business continuity plan in place? How frequently are restoration plans exercised and updated?
- ☐ Is there a plan for reporting on progress of network restoration? How frequently are these plans exercised?
- ☐ Is information related to network outages and restoration activity safeguarded and classified appropriately to mitigate security concerns?
- ☐ What is the single government point of contact for sharing communications outage and restoration information with other stakeholders? Having one point of contact can prevent duplication of effort on the operators' part.
- ☐ Has a forum for operators to share information and coordinate possible assistance been established? Consider the group's mandate, operational procedures or guidelines, and ways in which to utilize this forum.
- ☐ Consider whether a procedure could be put in place to allow the government to share sensitive threat information with network operators.
- ☐ What procedure is in place to assist operators with critical items such as physical access and expedited fuel deliveries?

Simple scoring approach to the checklist

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
	I. NATIONAL GOVERNMENT: ROLES, RESPONSIBILITIES & COORDINATION PROVISIONS		
1.	Is there a designated government ministry/agency responsible for disaster management in the country?		
2.	Does the lead disaster management ministry/agency coordinate with other relevant ministries across government for disaster management?		
3.	Are there any ICT-specific legislations or mandates which enable the ICT ministry/agency and the national ICT regulator, to respond to certain aspects of preparedness and response?		
4.	Is there a standard operating procedure in place, outlining the role and mandate of the ICT ministry/agency and regulator, with regards to preparedness and response?		
5.	Are there clearly defined points of contact established for disaster management in the respective agencies/ministries involved?		
6.	Can key contacts (identified in question 5) be reached at any time of the day or night?		
7.	Is there a national emergency telecoms cluster group established, representing key ICT contact persons?		
8.	Does the core ICT contact group meet yearly to coordinate and/or conduct drills/exercises?		
9.	Are roles, goals, and responsibilities coordinated across national to sub-national and community levels?		
10.	Are there mechanisms that help emergency response agencies and policymakers to plan and implement interoperability solutions for data and voice communications including governance, standard operating procedures (SOPs), technology, training and exercises, and usage of interoperable communications?		
11.	Are there methods/tools that jurisdictions that can be used to track progress in strengthening interoperable communications across the country?		
12.	Is telecommunications/ICT prioritized, or addressed, as a critical function or priority within the country's disaster management framework?		
13.	Does the communications ministry/agency or regulator coordinate with, and participate in, the activities of the national disaster management agency?		
14.	Has a national-level ICT Working Group been established?		
15.	Does the national ICT Working Group meet regularly?		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
16.	Has an up-to-date national ICT capacity assessment been done, which covers macro and micro assessments of country-level ICT infrastructure?		
17.	Is there an updated available list of telecommunications, information technology (IT), payment technology, and payment switch providers?		
18.	Are relevant tools available for rapid beneficiary registration and assistance delivery?		
19.	Is a roster of national IT service providers available and accessible?		
20.	Have network operators identified their internal "surge capacity", to be able to recover post-disaster?		
	PERCENTAGE = (Sum of Yes responses)/20 X 100		
	II. EXTERNAL COORDINATION WITH KEY STAKEHOLDERS		
21.	Is there a stakeholder engagement plan in place for disaster preparedness and response?		
22.	Is there a regularly updated list of key points of contact for primary organizations working in disaster risk management (including government private sector, civil society, United Nations, and all key others)?		
23.	Is the list of key point of contact shared with these entities (mentioned in question 22)?		
24.	Are these multiple stakeholders (mentioned in question 22) coordinated with frequently for preparedness and response readiness activities and actions?		
25.	Do key stakeholders have the ICT tools needed to communicate during non-disaster periods and emergency operations?		
26.	Are citizens involved in disaster risk reduction and response initiatives?		
27.	Are citizens informed about disaster response preparedness and plans?		
28.	Are there any requirements or legislations governing stakeholder engagement, public outreach, or advisory committees?		
29.	Have processes been established in advance for both the entry of experts and communications equipment in times of disaster, such as the ratification of the Tampere Convention?		
30.	Is there a fast-track process for importation of telecoms equipment in times of emergency?		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
31.	Are persons with disabilities, specific needs, and other vulnerable groups, included in disaster preparedness activities?		
	PERCENTAGE = (Sum of Yes responses)/11 X 100		
	III. CAPACITY DEVELOPMENT: TRAININGS AND SIMULATION EXERCISES		
32.	Is ICT-specific training or certification mandatory for officials who are involved in disaster risk management?		
33.	Do such trainings (mentioned in question 32) take place regularly?		
34.	Do ICT-specific trainings and exercises include different concerned key stakeholders, in addition to government participants?		
35.	Are telecommunication drills conducted to ensure that the public is aware of disaster response plans, including the most efficient means of communications to help reduce network congestion, together with recognition and reaction to a warning signal (e.g., response to an early warning mechanism such as a siren)?		
36.	Has a personal communications plan for family check-ins and evacuations been prepared?		
37.	Are communications/ICT exercises conducted, as part of more comprehensive national disaster exercises?		
38.	Are communications/ICT exercises tailored to the types of frequently occurring disasters in the country?		
39.	In communications/ICT exercises, are complex emergencies considered that could address multiple hazards in a “worst case scenario”?		
40.	Do other government agencies or ministries oversee and/or participate in communications-related exercises or drills?		
41.	Are different non-government stakeholder participants in disaster response or disaster communications exercises?		
42.	Do all the ICT sector stakeholders participating in disaster exercises or drills have clearly defined roles and responsibilities?		
43.	Are outage reporting requirements of carriers exercised?		
44.	Do carriers follow a uniform reporting process, and know which contacts to report the outages (induced by disaster) to, and how?		
45.	Is online ICT training, or are “read-aheads”, available for ICT stakeholders prior to exercises?		
46.	Is feedback collected after exercises or drills to help improve procedures or performance for the future?		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
47.	Is an "after action" performed after an exercise or drill?		
	PERCENTAGE = (Sum of Yes responses)/16 X 100		
	IV. INFRASTRUCTURE AND TECHNOLOGY: REQUIREMENTS, PLANNING AND MAINTENANCE		
48.	Is a regular technology inventory or assessment undertaken?		
49.	Does such an inventory or assessment (as mentioned in question 48) have a mapping of infrastructure and networks available (publicly)?		
50.	Is redundancy and resiliency planning undertaken for telecommunication providers?		
51.	Are there opportunities to support or encourage telecommunication operators in doing the redundancy and resiliency planning? This could include advisory efforts, opportunities to engage in drills and exercises, and after actions, information-sharing efforts.		
52.	Are processes in place for the government to help expedite, facilitate, prioritize, or enable fuel delivery for communications network generators?		
53.	Are there available and pre-positioned power sources for telecommunication networks?		
54.	Are there guidelines in place for critical facilities to have back-up power supplies?		
55.	Are regular technical trainings conducted for those personnel who will need to use and maintain/test emergency communications equipment, particularly that which is pre-positioned?		
56.	Do first responders know where the pre-positioned equipment is located or where imported ICT equipment can be collected for use?		
57.	Are local communities and local staff also considered for training in the use and maintenance of emergency telecommunications equipment?		
58.	Have critical /priority telecommunication sites being identified for restoration?		
59.	Are there mechanisms in place to prioritize critical telecommunication sites for restoration efforts?		
60.	Are related reporting mechanisms in place?		
61.	Has there been an assessment of ICT regulatory and/or policy barriers to entry or operation of needed equipment for disaster relief or restoration of networks?		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
62.	In the above-mentioned ICT assessment (question 61), have special measures been determined in case of an emergency, including identification of equipment for replacement, sources for rapidly sourcing equipment in times of need, determining redundant backup systems, and logistics capacity?		
63.	Is connectivity information, including data sets, available for government or public use to aid in disaster response and risk reduction planning?		
64.	Is information about business continuity plans exchanged between government and industry officials?		
65.	Have emergency and network resilience/redundancy needs and requirements been considered in the national telecommunications development plan?		
66.	Are policies in place to ensure that data can be shared by operators with responders in a way that protects individual privacy, while enabling response?		
67.	Are multiple channels (such as television, Radio, Short Message Service, messaging, etc.) employed to ensure information gets to those affected quickly and effectively?		
68.	Is social media employed to share information regarding disaster risk reduction?		
69.	Are regular/ongoing national and regional alerting exercises and system-testing taking place?		
70.	Is public education undertaken to sensitize communities on early warning for early action?		
71.	Are members of vulnerable populations consulted regarding their specific needs in disaster scenarios?		
72.	Is there an early warning alerting system in place?		
73.	Is the Common Alerting Protocol (CAP) employed for early warning purposes?		
74.	Are information materials including websites or applications (“apps”) accessible for disaster preparedness?		
75.	Are the above-mentioned “apps” (in question 74) promoted widely to the public?		
76.	Are information materials being shared in advance on ways that users of communications can lessen network congestion in a disaster?		
77.	Are ICT capacities of vulnerable populations being developed in disaster risk management?		
78.	Are accessibility and usability of ICTs considered in forthcoming disaster preparedness projects?		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
79.	Are disaster readiness information materials provided targeting vulnerable populations?		
80.	Are public awareness campaigns conducted on disaster risk reduction themes in multiple accessible formats in different prevalent languages?		
81.	Following a disaster, are disaster response efforts reviewed to assess challenges for vulnerable groups, and determine follow up actions?		
	PERCENTAGE = (Sum of Yes responses)/34 X 100		
	(a) ICT assessment and damage mitigation		
82.	Is there a designated focal point at the ministry/regulator to collect, analyse, and react to/report/release information regarding damage to networks?		
83.	Is a mechanism in place to enable communications operators to provide the government information about the scale and scope of communications outages, and their progress on restoration in a way that enables governments to plan and act?		
84.	Is the reporting system separate or "firewalled" from regulatory functions to enable more open reporting on outages?		
85.	For those networks that are commercial or public, are there reporting requirements in place that would establish a harmonized process, format, and timeline carriers to submit evaluations?		
86.	Will initial damage assessments be connected to award disaster recovery funding?		
87.	Have interagency coordination and information sharing processes been established?		
88.	Are there policies in place that consider communications network status, needs, conditions and requests, and that enable the maintenance and restoration of the following communications capabilities?		
89.	Is standardized reporting on outages undertaken by the regulator at regular intervals, identifying the number of telecommunication sites that are up and/or down?		
90.	Are telecoms recovery plans produced, to recover or continue the operation and use of telecoms infrastructure in the event of disaster?		
91.	Do the above-mentioned telecoms recovery plans (in question 90) detail coverage areas and network carrying capacity – including provision of special services and network access for affected areas?		

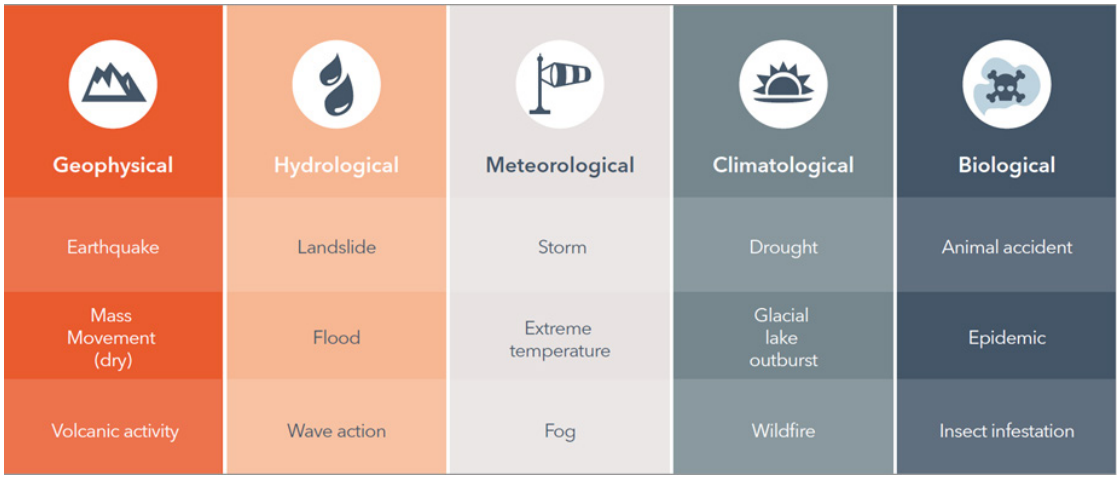
No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
92.	As a business continuity management (BCM) measure post-disaster, are network recovery mitigation plans made available by network operators, and are accessible?		
	PERCENTAGE = (Sum of Yes responses)/11 X 100		
	(b) Emergency connectivity provisions & approach		
93.	Has the government identified relevant network operators and service providers, including domestic telecommunications providers and international satellite operators, who may be involved in providing emergency communications services?		
94.	Is there a maintained list containing updated details for all relevant telecoms service provider recovery teams?		
95.	Is there a system in place for offers of financial and human capacity assistance from foreign governments, humanitarian organizations, or private sector to be received and processed?		
96.	Is the ICT ministry or regulator the contact for authorization of incoming equipment (such as frequency and type approvals), or to allocate requested frequencies?		
97.	Has the government created frequency allocations, in conformance with the international table of allocations, for critical satellite communications frequency bands – including in the L, C, Ku, and Ka bands?		
98.	Is there a mechanism to ensure timely coordination with local operators to avoid interference?		
99.	Are emergency ICT resources prepositioned at priority locations?		
100.	Does the government encourage or enable carriers to preposition emergency ICT resources?		
101.	Is there a process in place for regular tests of the pre-positioned equipment to ensure its functionality?		
102.	Is consideration/priority given to fuel supplies for power generators and restoration of telecommunication networks?		
103.	Is coordination between national government-specific telecommunications teams and the central disaster management institutions undertaken?		
104.	Is there a prioritization exercise undertaken to determine where emergency connectivity will first be established?		
	PERCENTAGE = (Sum of Yes responses)/12 X 100		
	(c) Network maintenance and reestablishment		

No.	Question	Response [Yes/No] Y=1; N=0	Comments [Qualifying]
105.	Is there a source of external expert advice and assistance for government agencies, with respect to restoring government communications networks and telecommunication infrastructures, including industry contacts?		
106.	Does the government have mechanisms or emergency procedures in place to facilitate customs clearance or importation of equipment needed for restoration of critical networks, and/or to facilitate entry of any external expert personnel needed to restore and rebuild networks?		
107.	In case of pre-positioned equipment, has a focal point (or points) been identified to ensure it is well-maintained, and the ICT equipment is ready-for-use in an emergency?		
108.	Is there a process in place to routinely test networks designed for emergency communication?		
109.	Are commercial or public network operators encouraged to have a business continuity plan (BCP) in place?		
110.	Are telecommunications restoration plans frequently exercised and updated?		
111.	Does the ICT ministry/agency or regulator have information related to network outages and restoration activity safeguarded, and classified appropriately, to mitigate security concerns?		
112.	Does the ICT ministry/agency or regulator have a focal point for sharing communications outages and restoration information with other stakeholders?		
113.	Has a forum for operators to share information and coordinate possible assistance been established by the ICT ministry/agency and/or regulator?		
114.	Has a procedure been put in place to allow the government to share sensitive risk-related information with network operators (and vice versa)?		
115.	Is there a procedure in place to assist operators with critical items, such as physical access and expedited fuel deliveries?		
116.	Are there alternate sources of power located and prepared in case of emergency scenarios?		
	PERCENTAGE = (Sum of Yes responses)/12 X 100		

Annex B: Types of disasters

Given that there is a need to conduct a risk analysis to establish the vulnerability of a given country before establishing a national disaster risk management plan, this annex addresses variation in the types of disasters, as classified by the Center for Research on the Epidemiology of Disasters (CRED).[1] CRED categorizes disasters as climatological, geophysical, hydrological, meteorological or technological, among other categories.[2]

Figure B1: Disaster categories according to CRED



Source: Based on CRED (2017). Annual Disaster Statistical Review 2016.

Climatological disasters

Climate-type disasters refer to those caused by long-lived, meso- to macro-scale atmospheric processes ranging from intra-seasonal to multidecadal climate variability.[3]

Examples of climatological disasters include droughts and wildfires. A drought can be defined as a "prolonged absence or marked deficiency of precipitation,"[4] or as "a period of abnormally dry weather sufficiently prolonged for the lack of precipitation to cause a serious hydrological imbalance".[5] The resulting impacts of such an imbalance – such as crop damage or a scarcity of water used by people, animals or plants – can lead to consequences as serious as death.[6]

Wildfires, on the other hand, are defined as "any uncontrolled and non-prescribed combustion or burning of plants in a natural setting such as a forest, grassland, brush land or tundra, which consumes natural fuels and spreads based on environmental conditions (e.g., wind, topography)."[7]

1 EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).
2 Other categories of disaster include those of a biological nature, defined as caused by exposure to living organisms and their toxic substances; and alien type, defined as those caused by asteroids, meteoroids and other extraterrestrial objects when they pass nearby, enter the atmosphere and/or hit the Earth, or by changes in the interplanetary conditions affecting the magnetosphere, ionosphere and thermosphere of the Earth. Source: CRED.
3 EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).
4 World Meteorological Organization – Meteoterm (https://public.wmo.int/en/resources/meteoterm).
5 Ibid.
6 American Red Cross (www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies.html).
7 EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).

Geophysical disasters

These types of disasters originate from activity of the Earth, according to the classification of CRED. They can include earthquakes, whether on land or under the seabed; volcanic activity; and sudden terrestrial movements.[8]

Earthquakes are defined as a "vibratory motion of the ground of a random nature resulting from the propagation of a disturbance originating inside the Earth's crust."[9] Earthquakes can occur both on land and below the ocean floor, and in the latter case can generate large ocean waves or tsunamis.[10] A volcano, on the other hand, can be defined as "a vent or fissure in the Earth's surface from which lava and volatiles are extruded."[11]

The third type of disaster of geologic origin is the mass movement of large amounts of terrestrial material, including any type of downward movement of ground material. These threats include avalanches, landslides and rock falls.[12]

Hydrological disasters

Hydrological disasters are those caused by changes in the movement and distribution of surface and subsurface fresh water and salt water. Such disasters can cause flooding, whether coastal floods (higher-than-normal water levels along the coast caused by tidal changes or storms); river floods (due to sudden, heavy rainfall, usually associated with temporary weather events); or ice jam floods (accumulation of floating ice restricting or blocking a river's flow and drainage).[13]

Another hydrological-type disaster is a seiche, which refers to an "oscillation (lasting from a few minutes to several hours) of the surface of a lake or other small body of water caused by minor earthquakes, winds, or variations in atmospheric pressure".[14]

Meteorological disasters

The term *meteorological disasters* refers to the hazards caused by short-lived, micro- to meso-scale extreme weather and atmospheric conditions that last from minutes to days.[15] These include extreme temperatures, fog (small drops of water suspended in the air near the surface of the Earth) and storms.

Extreme temperatures include heat waves, cold waves, and severe winter conditions.[16] A storm is defined as "an atmospheric disturbance involving perturbations of the prevailing pressure and wind fields, on scales ranging from tornadoes (1 km across) to extratropical cyclones (2 000–3 000 km across)."[17]

---

8 Ibid.
9 World Meteorological Organization – Meteoterm (https://public.wmo.int/en/resources/meteoterm).
10 American Red Cross (https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies.html).
11 World Meteorological Organization – Meteoterm (https://public.wmo.int/en/resources/meteoterm).
12 EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).
13 Ibid.
14 World Meteorological Organization – Meteoterm (https://public.wmo.int/en/resources/meteoterm).
15 EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be/Glossary).
16 Ibid.
17 World Meteorological Organization – Meteoterm (https://public.wmo.int/en/resources/meteoterm). Extreme weather events are known as hurricanes, typhoons or tropical cyclones depending on the region of the world in which they occur.

Biological Disasters

Biological Disasters are a type of natural disaster that emerges from exposure to living organisms and related toxic substances or diseases. Contained within this category are epidemics, including for example the Spanish influenza or the 2019/2020 Covid-19 pandemic, as well as hazards related to animals and plants, such as mosquito borne infections, insect infestations, and venomous plants or animals. With regard to epidemics in particular, this can refer both to diseases that have rapidly increased in prevalence in areas or among populations where they already previously existed, as well as to the emergence of a new disease that was not present previously.[18]

Technological disasters

Finally, technological-type disasters are those caused by hazards of human origin, such as industrial, transport, or other types of accidents, including fire, collapse or explosion of physical infrastructure, and any other technological disaster that is not considered an industrial or transport accident.[19]

[18] International Federation of Red Cross and Red Crescent Societies- IFRC- Biological hazards: epidemics https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/definition-of-hazard/biological-hazards-epidemics/

[19] The Emergency Events Database – Université Catholic De Louvain (UCL) – CRED (https://www.emdat.be/classification).

Annex C: Historical disasters by region[1]

Table C1 presents a summary of the disasters that occurred from 1968 to 2017, categorized by continent and type of disaster described in the sections above. The Table summarizes the number of events that occurred, the number of fatalities and injured, the total number of people affected, and the number of people left homeless after the emergency.

Table C1: Disasters over the 50-year period 1968–2017

Type of disaster	Events	Fatalities	Injured	Affected	Homeless	Total affected
Africa						
Climatological	249	505 166	758	361 810 319	32 088	361 843 165
Geophysical	48	2 805	4 224	271 606	253 285	529 115
Hydrological	783	18 178	10 174	56 480 704	3 841 495	60 332 373
Meteorological	212	4 919	14 116	15 944 315	1 852 465	17 810 896
Technological	1 518	56 335	34 624	373 270	216 811	624 705
Total Africa	**2 810**	**587 403**	**63 896**	**434 880 214**	**6 196 144**	**441 140 254**
Americas						
Climatological	292	450	1 637	109 850 315	64 935	109 916 887
Geophysical	299	369 876	675 968	31 476 615	4 274 214	36 426 797
Hydrological	1 221	70 278	55 394	93 387 582	3 801 134	97 244 110
Meteorological	1 240	62 437	1 877 928	152 702 945	3 743 926	158 324 799
Technological	1 301	42 394	57 526	3 213 955	30 237	3 301 718
Total Americas	**4 353**	**545 435**	**2 668 453**	**390 631 412**	**11 914 446**	**405 214 311**
Arab States						
Climatological	65	189 701	15	62 291 213	20 000	62 311 228
Geophysical	37	8 395	33 693	1 399 553	742 234	2 175 480
Hydrological	273	10 965	22 307	12 494 389	2 945 145	15 461 841
Meteorological	73	1 234	6 195	4 188 485	55 960	4 250 640
Technological	714	33 129	25 271	18 988	22 835	67 094
Total Arab States	**1 162**	**243 424**	**87 481**	**80 392 628**	**3 786 174**	**84 266 283**
Asia–Pacific						
Climatological	239	6 536	1 919	2 000 231 872	93 181	2 000 326 972
Geophysical	694	912 236	1 577 007	127 624 985	14 871 692	144 073 684
Hydrological	2 159	253 328	1 245 812	3 463 735 595	79 419 927	3 544 401 334
Meteorological	1 723	773 882	794 663	949 398 926	41 851 503	992 045 092

[1] EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be). All figures belong to the period 1968–2017.

Type of disaster	Events	Fatalities	Injured	Affected	Homeless	Total affected
Technological	3 312	138 405	220 327	1 812 985	680 470	2 713 782
Total Asia–Pacific	**8 127**	**2 084 387**	**3 839 728**	**6 542 804 363**	**136 916 773**	**6 683 560 864**
Commonwealth of Independent States						
Climatological	38	171	2 319	8 031 194	3 855	8 037 368
Geophysical	42	2 254	2 811	1 027 017	92 086	1 121 914
Hydrological	162	3 731	8 736	5 081 279	306 524	5 396 539
Meteorological	70	58 379	8 876	6 187 536	28 900	6 225 312
Technological	276	8 108	5 218	25 626	10 410	41 254
Total Commonwealth of Independent States	**588**	**72 643**	**27 960**	**20 352 652**	**441 775**	**20 822 387**
Europe						
Climatological	126	537	1 213	10 233 832	8 505	10 243 550
Geophysical	168	38 657	118 580	7 626 303	1 688 938	9 433 821
Hydrological	586	6 075	6 145	13 356 770	442 175	13 805 090
Meteorological	665	89 734	23 720	8 684 741	17 603	8 726 064
Technological	855	26 714	51 794	136 976	202 766	391 536
Total Europe	**2 400**	**161 717**	**201 452**	**40 038 622**	**2 359 987**	**42 600 061**
World total	**19 440**	**3 695 009**	**6 888 970**	**7 509 099 891**	**161 615 299**	**7 677 604 160**

Definitions:

- Events: Number of times a disaster occurred.
- Fatalities: Number of people who lost their lives.
- Injured: Number of people suffering physical injuries, trauma and/or illness requiring immediate assistance.
- Affected: Number of people requiring immediate assistance during an emergency period, *i.e.*, requiring assistance to meet basic survival needs such as food, water, shelter, sanitation and immediate medical assistance.
- Homeless: Number of people whose homes were destroyed or severely damaged, and therefore required shelter after the disaster.
- Total affected: Corresponds to the sum of injured persons, affected and homeless after a disaster.

Source: EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).

Over the last five decades, 19 440 disaster events were recorded worldwide,[2] which caused more than 3.6 million fatalities, with almost twice as many people injured and a total of more than 7.5 billion people affected.[3] Although technological, hydrological and meteorological disaster types were most common (7 976, 5 184 and 3 983 events, respectively), geophysical disasters caused the highest number of deaths (1.33 million). Almost half the total number of people affected by disasters during the past 50 years (48.5 per cent) were affected by hydrological disasters, while meteorological disasters generated the highest proportion of people injured (39.6 per cent).

[2] The figures presented throughout the document only consider the five types of disasters described in Annex B.

[3] EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).

The Asia–Pacific region was the region with the largest number of reported disaster events (8 127), almost 4 000 events more than in the Americas. The Asia–Pacific region also had the highest number of fatalities (2.1 million), more than triple the nearly 600 000 deaths recorded in the Africa region, as explained below.

Africa[4]

The Africa region reported 2 810 disaster events of natural and technological origin from 1968 to 2017. In these disasters, 587 403 people lost their lives and almost 435 million were affected. The economic losses produced by these emergencies reached a total of USD 27.3 billion (in 2017 dollars).

Based on the data reviewed, climatological, hydrological and technological disasters such as droughts, floods and transport accidents represent the greatest vulnerability for countries in the Africa region in terms of frequency, fatalities and total number of people affected.

Americas[5]

From 1968 to 2017, there were 4 353 disaster events that occurred in the Americas region caused by natural and technological hazards. These disasters caused 545 535 people to lose their lives, more than 390 million to be directly affected, and economic damage estimated at USD 1.8 trillion (in 2017 dollars).

The disasters that occurred most frequently were storms, followed by floods and transport accidents. Although storms occurred most frequently, nearly two-thirds of the fatalities in the continent were caused by earthquakes.

These events, along with a volcanic eruption in 1985 and a flood in 1999, which caused almost 22 000 and 31 000 fatalities, respectively, suggest that the Americas region is vulnerable to multiple types of disasters. This includes both geophysical, which cause the most significant impact on human life, and hydrological and meteorological disasters, which occur more frequently and affect a larger portion of the population.

Arab States[6]

More than 1 100 emergency events occurred in the Arab States region during the last 50 years. As a result, more than 240 000 people were killed, almost 90 000 were injured, more than 80 million people were affected, and the economic losses reached USD 53.6 billion (in 2017 dollars).

Even though technological and hydrological emergencies were the most frequent in these countries, with 714 and 273 cases, respectively, the climatological hazards were the ones that took more human lives (78 per cent of the total death toll in the region) and that affected the most people (74 per cent of the total affected).

Asia–Pacific[7]

In the Asia-Pacific region, the 8 127 disaster events that occurred from 1968 to 2017 caused 2 084 387 fatalities, affected more than 6.5 billion people, and generated economic loss of around USD 1.9 trillion (in 2017 dollars).

Almost half of the fatalities (44 per cent) were caused by geophysical disasters, such as earthquakes or tsunamis, despite the fact that technological disasters were the most frequent emergency event in the region, with 3 312 individual cases. These facts suggest that earthquakes and tsunamis are the greatest sources of vulnerability in the region and have the greatest impact on the population (cases

4 Based on EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).
5 Ibid.
6 Ibid.
7 Ibid.

in China, Indonesia, Islamic Republic of Iran, Pakistan, Sri Lanka, etc.).[8] However, of the six disasters with the highest number of casualties in the region during the period, three were storms, which in 1970, 1991 and 2008 caused more than 590 000 fatalities.

Commonwealth of Independent States[9]

For this group of countries, the 588 disasters reported from 1968 to 2017 caused the deaths of 72 643 people, left almost 28 000 people injured, and affected more than 20 million people. The economic losses reached USD 20.5 billion (in 2017 dollars).

Of the total death toll, 80.4 per cent were caused by meteorological hazards, even though only 70 such events were reported. The 276 technological disasters that occurred in the same period killed more than 8 000 people (11.2 per cent) and affected nearly 40 000 (0.2 per cent). Climatological hazards, on the other hand, even though less frequent in the Commonwealth of Independent States, are the type of hazard that affects the most people, with more than 8 million during the period under study.

Europe[10]

In Europe, the 2 400 disaster events recorded from 1968 to 2017 caused 161 717 fatalities, affected more than 40 million people, and caused almost USD 628 billion (in 2017 dollars) in economic losses.

The most frequently occurring disasters were technological, with 855 cases, although extreme temperatures were the cause of nearly two-thirds of the total disaster-related death toll in the region.

8 PreventionWeb (www.preventionweb.net/english/countries/statistics/index_region.php?rid=5).

9 Based on EM–DAT, the Emergency Events Database. Université Catholic De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels (www.emdat.be).

10 Ibid.

Annex D: Additional information on telecommunication/ICTs for emergencies[1]

This annex describes in more detail the different public and private telecommunication/ICT services – including radio and television (TV) broadcasting services, among others – that should be considered in the development of an NETP.

Telecommunication/ICT services

The term *public services* refers to services offered through telecommunication/ICT networks to which ordinary citizens have access, while the term *private services* refers to services offered through telecommunication/ICT networks to which specialized users – such as police, fire brigades, civil protection authorities, government authorities or private companies, among others – have access. This section also describes Internet and social networks, amateur radio and broadcasting services, and their use in relation to disaster management.

Public telecommunication/ICT services

Public telecommunication/ICT services, such as voice and data, are provided through three different types of telecommunication network: fixed, mobile and satellite.

Public telecommunication/ICT services via fixed networks

Fixed networks (e.g., the Public Switched Telephone Network) connect the subscriber through the local wireline or fibre distribution network – also known as local loop or last mile, with the local exchange – or through the wireless local loop network (WLL) with a radio base station (RBS). In turn, local exchanges are connected with other local exchanges within a city, or through interurban lines for routing long distance calls.

The wireline local loop has advantages and disadvantages in the event of a disaster or an emergency:

> Disadvantages: In many countries, telephone networks are mainly deployed on poles, which are vulnerable to catastrophes caused by earthquakes and strong winds. The fall of a pole can interrupt the circuit and leave the service inoperable for a considerable period, depending on the damage to routes used to access the infrastructure.
>
> Advantages: If the power supply is interrupted, the telephone service will continue to function, because it is powered by a battery at the telephone exchange. Although this advantage is lessened, as many countries are moving to locally powered systems such as Internet Protocol-based networks that replace analogue networks, there are still countries using centrally powered systems, e.g., least developed countries, which could take advantage of centrally powered systems.

The installation of cables in underground ducts helps overcome these disadvantages and reduces the vulnerability of this type of network. On the other hand, the advantage of this type of network is limited by the common use of cordless telephones in the home, whose base station is powered by energy from the power distribution network. Therefore, it is recommended to have at least one telephone powered by the battery at the telephone exchange or to acquire a cordless telephone that includes a battery in the base station that can power the network interface, allowing functionality during a power outage.

In the case of WLL, the subscriber's connection is made through a radio link between the RBS and the radiocommunications equipment in a fixed location (such as a home or office), which in turn is connected to the subscriber's telephone. Even though WLL is less vulnerable to damage to poles, on which the wireline telephone networks depend, it is dependent on the power distribution network.

---

[1] These sections are mainly based on ITU (2007a), *Compendium of ITU work on Emergency Telecommunications*. It is recommended to refer to said document for additional information on any of the topics presented.

When power supply is interrupted, the communication service is also interrupted, because the radiocommunications equipment in the home will not be able to work.[2] On the other hand, if the RBS has an alternative power source and is connected to the telephone exchange through local cable networks or microwave links, as is sometimes the case, the network might be less vulnerable to certain types of disasters that knock out traditional ICT infrastructure, such as utility poles.

The telephone or local exchanges are the basic element of the telephone systems mentioned above. In a possible emergency or disaster, different types of risks or failures can present themselves:

- Call congestion: Because the exchanges are designed to simultaneously receive calls of typically no more than 5 per cent of subscribers in residential areas and 10 per cent in commercial areas, when the number of simultaneous calls surpasses these thresholds, the local exchange is blocked, and it is not possible to route calls.
- Power supply interruption: If the supply of power from the power distribution network is interrupted and, in addition, back generators or batteries fail, it is likely that all telecommunication/ICT services provided through said local exchange, including voice and data (Internet), will be interrupted.
- Building collapse: The collapse of the building hosting the local exchange can be the result of various natural hazards, such as floods, earthquakes, etc. In this case, the telecommunication/ICT services are interrupted indefinitely for those subscribers who are connected to said local exchange.

To minimize the above-mentioned risks, the following actions should be considered:

- Prioritize access by high-priority users to the available capacity when the local exchange is congested. It is possible to carry out this prioritization through three strategies:

  1. Block all low-priority users, denying general subscriber access to the service.
  2. Allow high-priority users to avoid the queue and obtain the next available circuit.

  The implementation of any of these options should be coordinated with regulatory entities. In fact, in many cases, the regulatory authority defines the strategy to be implemented.
- In order to mitigate the need to make difficult decisions regarding blocking or eliminating particular users, authorities could promote educating consumers and carriers on ways to lessen network congestion[3].
- Install alternative sources of power using solar/gas/diesel/petrol-based generators. In such a case, it is necessary to establish a plan that allows the supply of fuel in the proper amount so as not to have subsequent interruptions.
- Local exchanges should be located in areas with minimal exposure to natural hazards or where the structure and construction of structures is adequate to support them, for example, through anti-seismic constructions.

Finally, long-distance links between exchanges are required and are typically made through fibre-optic, microwave or wired networks. In microwave links, relay stations are often installed in hills or tall buildings. However, these are typically in exposed places, where wind may cause misalignment of antennas or destruction of towers, or in distant areas that are difficult to access.

In the event of a disaster, the difficulty of reaching these areas may delay the restoration of service. In this regard, the government should initiate plans to expedite access to remote relay stations. Additionally, a way to avoid the interruption of communications in these cases is with the installation of redundant routes or links that can be an alternative if the primary route fails. The regulator should strive to promote adequate redundancy systems.

[2] Unless there is an alternative power supply, e.g., UPS, which is not common.
[3] See more at: https://www.fcc.gov/reports-research/guides/tips-communicating-emergency

Public telecommunication/ICT services via mobile networks

Mobile broadband subscriptions have grown more than 20 per cent annually in the last five years, reaching 4.3 billion subscriptions in 2017, *i.e.*, almost 60 per cent penetration (ITU, 2017b). Similarly, mobile cellular subscriptions reached more than 7.6 billion in 2017, *i.e.*, more than 100 per cent penetration. Thus, mobile networks and services have spread throughout the world and therefore are key in responses to emergency events.

In mobile networks, telecommunication/ICT services are provided through an extensive network of terrestrial RBSs. These networks are designed to optimize the coverage and capacity of the network. Generally, the RBSs are in the areas with the highest population density and consequently with the highest volume of traffic, *i.e.*, in urban areas. However, with the introduction of fourth-generation systems and the use of spectrum bands below 1 GHz, mobile networks are able to cover rural areas more efficiently.[4] Nevertheless, there are still obstacles to establishing mobile communications in remote and rural areas, and these are made worse in the event of emergencies or disasters. This is especially true in developing countries, where it is difficult to establish a business model that is financially viable to cover rural or otherwise remote geographic zones.

Mobile networks, in the same was as fixed networks, also have capacity problems, insofar as they are designed to provide service to only a portion of total users simultaneously. When network usage is at or above the maximum, the network becomes congested.

RBS for mobile networks are connected to mobile exchanges through microwave links, optical fiber, or wired networks, similar to fixed networks. Likewise, mobile exchanges are also vulnerable to power failure and will only remain operational for the period that their on-site batteries and back-up generators last.

There are also so-called *cells on wheels* or COW radio base stations. These are mobile base stations that can be rapidly installed in specific locations to increase coverage and capacity when required or to replace an RBS that has been destroyed. The speed at which COWs can be installed, nonetheless, depends very much on the accessibility of the specific locations. Earthquakes, floods, mudslides, and other disasters can make roads impassable and thereby prevent deployment of COWs to the desired locations.

During an emergency or disaster, mobile networks, similar to fixed networks, can prioritize use of the network through the mobile exchange to assign a preferential capacity to specific users, to allow these users to make calls even in congested conditions. The regulatory authority must establish who should belong to the group of users with preferential capacity.

When networks provide SMS and third- and fourth-generation data services, it is recommended to maintain service by slowing network speeds (storage and retransmitting), as opposed to completely blocking users. In fact, in an emergency or disaster event, prioritizing SMS and data services such as e-mail or messaging-over-voice services can help avoid network congestion, because these services use network capacity more efficiently.

Finally, alerts can be disseminated widely through text message, mobile apps or social media via mobile systems, allowing messages warning the public of possible risks or emergency events and possible disasters, to quickly reach a large number of people. Social media, for example, has become a critical component in all four phases of disaster management. Information on emergency events witnessed by the public can be sent to public safety organizations through social media. In turn, public

[4] Frequencies below 1 GHz are optimal for covering rural areas because the radio-electric signal propagates over greater distances and consequently less infrastructure and lower costs are required to cover a specific area with voice and data services.

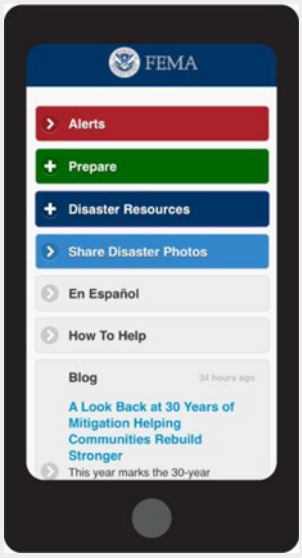
safety organizations can plan response strategies, and provide updated and accurate information to the public.[5]

Box D1: United States Federal Emergency Management Agency Mobile App[1]

The Federal Emergency Management Agency (FEMA) Mobile App helps people stay safe and know what to do before, during, and after disasters. With this simple and easy-to-use resource, users can:

- Receive emergency alerts for up to five locations nationwide.
- Share real-time notifications with loved ones via text, email and social media.
- Learn emergency safety tips for over 20 types of disasters.
- Prepare for disasters with an emergency kit checklist, emergency family plan, and reminders.
- Locate open emergency shelters and disaster recovery centres in their area.
- Toggle between English and Spanish (Note: alerts are only available in English)

Figure D1: FEMA Mobile App



[1] United States Federal Emergency Management Agency, available at www.fema.gov/mobile-app (accessed 22 February 2019).

Public telecommunication/ICT services via satellites

Terrestrial communications services through mobile or fixed networks can be seriously affected after a disaster. The communication towers, telephone exchanges, utility posts and power supply (on which the wired network relies) can all suffer faults that make communication impossible.

As a result of these vulnerabilities, non-terrestrial wireless solutions such as satellite networks are important. These networks provide communications services that have very little dependence on terrestrial infrastructure, since the "base" radio stations are located in Earth orbit.

[5] United States Department of Homeland Security (2013). This document contains several social media implementation methods.

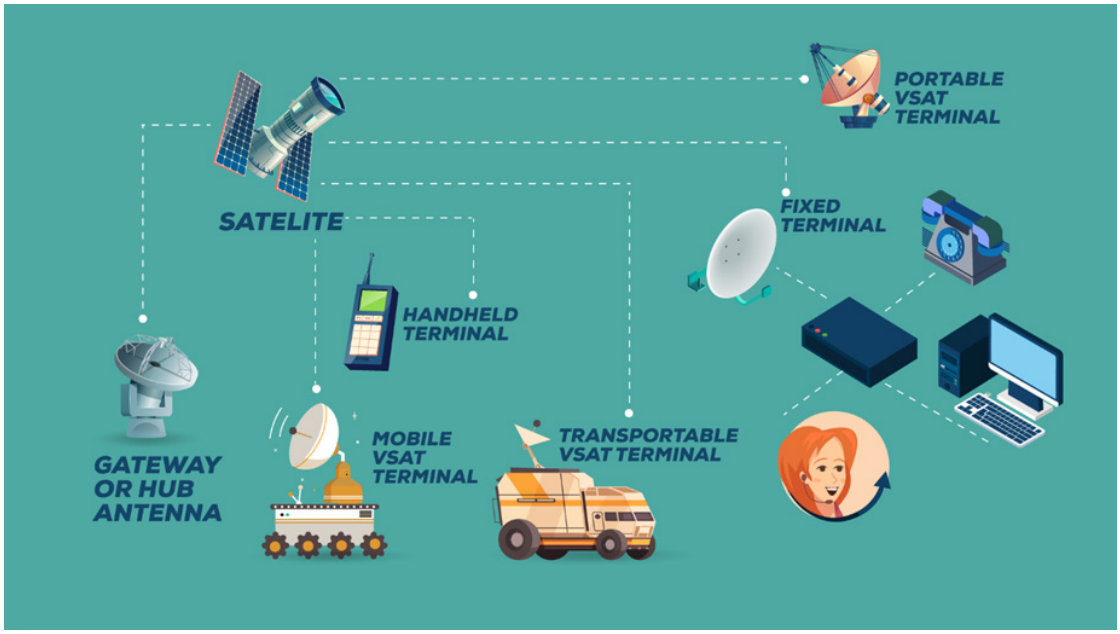
Nowadays, satellite networks provide various communications services: voice, data and video, through broadband connectivity, for example. These services can be classified into mobile satellite service (MSS) and fixed satellite service (FSS). Additionally, satellite services are classified into two types of systems: those that are in geostationary orbit, known as geostationary satellite systems; and those that are not (non-geostationary orbit), such as the satellite systems found in low-Earth orbit. Satellite terrestrial terminals range from gateways with large antennas located in a fixed location to small terminals the size of a mobile phone.

Satellite systems have the capability to offer fixed-to-fixed, mobile-to-mobile, fixed-to-mobile and point-to-multipoint communications, including interoperability with other communication solutions, e.g., land mobile radiocommunication services, mobile services, etc. Emergency response teams can be highly dependent on mobile satellite systems through the use of portable satellite phones and terminals, and applications such as mobile telephony, push-to-talk radio, emergency response coordination, messaging and data transfer, among others. Fixed satellite systems use terrestrial terminals at fixed locations, providing applications such as broadband Internet access, live video, telemedicine and videoconferencing, among others.

The development of high-throughput satellites—which has increased the efficiency of spectrum use, modulation, and spot-beam technology—has resulted in a substantial increase in available speed and capacity over a GSO satellite in the last decade. Today, GSO satellite providers are able to provide consumers in some regions of the United States of America with speeds of up to 100 Mbit/s. In addition, the non-geostationary orbit (NGSO) satellite constellations that are in the process of being planned and deployed will be able to offer high-speed service with low latency on a global basis. In addition, today there are also light weight easy to install satellite antennas, and WiFi connectivity through VSAT systems.

Portable or other transportable devices are useful for broadband communications that require voice, video and data applications. Finally, fixed satellite access equipment is used for various medium- and long-term operations: for example, monitoring and recovery systems after a disaster.

Figure D2: Satellite systems



Source: ITU

Private telecommunication/ICT services

Private telecommunication/ICT services provided through private networks are managed directly by the users of the network, such as firefighters, police, ambulances, relief teams, civil protection, transport, utilities, State authorities, ministries and defence, as well as other private sector entities. In some cases, networks are managed by third party operators who provide services to private clients. These private users can, in an eventual state of emergency, be asked to share these networks to support the emergency response.

The services that are presented through these networks can be mobile or fixed, whether wired or wireless. The classification of these services according to ITU is:

- land mobile radiocommunication (LMR) services;
- maritime services;
- aeronautical services;
- positioning services.

Below is a brief description of each of these services.

Land mobile radiocommunication services

LMR systems are the main systems used by public security agencies (e.g., police, civil defence and firefighters, among others) for public protection and relief operations. These systems, in which only one user can speak at a time by pressing the button to speak (push-to-talk), have been in use since the 1930s, evolving from conventional analogue systems, in which there are frequencies and channels assigned exclusively to groups of users for voice communications, to trunked digital systems, which are controlled by computer programs that assign a group of frequencies and channels for use by multiple individuals. These trunked systems allow the sharing of frequencies among a large group of individuals, increasing capacity and interoperability, reducing congestion of the network, and allowing a more efficient use of frequencies and communication channels. Likewise, there are LMR systems based on Internet Protocol, which further increases the capacity and the services offered – e.g., data – and improves interoperability.

LMR systems are important for the following reasons (United States Department of Homeland Security, 2016):

- They are the primary means of voice communications among public safety officials.
- They have evolved technologically to provide mission-critical functions.
- Security agencies have been trained in the use of LMR systems.

Likewise, as technologies evolve, there are a variety of systems that may be used by different agencies, some with conventional LMR systems and others with more advanced systems. This can present problems in some cases where the systems may not be compatible, preventing communication between different agencies using different systems.

On the other hand, agencies may be using systems in different bands of the radio spectrum, e.g., VHF and UHF or, more specifically, the 700 and 800 MHz bands. These systems do not always allow interoperability and therefore require additional investments to allow such interoperability.

LMR systems also offer a wide range of features: group, emergency, and/or prioritized calls and broadcasting; security features such as user authentication and end-to-end encryption; mobility features such as handover; voice features such as access priority, discrete listening and call duration limit, among others; data features such as access to databases, GPS location, messaging, file transfer, video transmission and others. The data transmission of these systems varies from 2.4 kbit/s up to several Mbit/s.

Maritime services

The Global Maritime Distress and Safety System is designed to increase safety, facilitate navigation and assist in the rescue of ships in distress through a set of safety procedures, equipment and communication protocols. This service is used only for boats and is regulated by the International Convention for the Protection of Human Life at Sea (SOLAS), approved by the International Maritime Organization, a specialized agency of the UN. The maritime radiocommunication service uses the frequencies that have been allocated for this purpose in the HF, MF and VHF bands for terrestrial systems: that is, communications between vessels and between vessels and ground stations.

Aeronautical services

These services are mainly to establish communications with aircraft from ground stations and between aircraft. For this purpose, different frequency bands have been allocated, e.g., in the 118–136 MHz band. The international emergency frequency is 121.5 MHz and uses amplitude modulation.

Positioning services

There are a number of global positioning and navigation systems worldwide, including (a) GPS, developed by the United States of America; (b) the GLONASS system (Global Navigation Satellite System), developed by the Government of the Russian Federation; and (c) GALILEO, a positioning system developed by the European Union that will be completed in 2019. These systems use a set of satellites and Earth stations to determine the position of a terminal, which must be in line of sight with the satellite: that is, in an open area.

This type of system is essential for rescue work in cases of emergency, because positioning equipment can help facilitate the search process. Likewise, periodic information on the positioning of rescue personnel can provide crucial data on the dangers that have been found in affected areas.

Additionally, logistics in the delivery of supplies and aid equipment can be facilitated through the use of GPS, especially when the transporters are unfamiliar with the area, or a disaster has affected the available transit pathways.

Internet

More than 50 per cent of the global population, *i.e.*, 3.9 billion people, used the Internet in 2018 by either mobile or fixed networks.[6] Social media such as Facebook, Instagram, WhatsApp, among others, will reach nearly 2.8 billion users worldwide in 2019.[7] Due to the widespread use of the Internet, it is a tool that supports operations and activities before, during and after a disaster. Access to the Internet is possible thanks to public telecommunication/ICT networks. In other words, it is not possible to access the Internet if there is no fixed or mobile telecommunication/ICT service, whether terrestrial or satellite. Therefore, in disaster situations where the communications service is affected, access to the Internet is also compromised. However, once the communications service has been restored, specifically the broadband data service, the Internet is a fundamental tool for dealing with disasters.

It is possible to access through the Internet information resources and applications that support disaster management activities. The following are some of these ways:

- e-mail;
- weather information;
- news;
- consultation of medical databases;

[6] ITU World Telecommunication/ICT Indicators database, available at https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx (accessed 22 February 2019).

[7] Statista, available at www.statista.com (accessed 22 February 2019).

- registering refugees and displaced persons;
- sending relevant information;
- general information.

The advantages of these information media are the speed at which media on the Internet can be shared and updated – including, for example, photos, graphics, audio, video, live video and other relevant information – and that people can subscribe to notification systems that send messages relevant to emergency situations. On the other hand, the disadvantages are mainly that information on the Internet is not updated in real time in disaster situations where Internet access cannot be guaranteed, or that information may be only updated at certain times (United States Federal Emergency Management Agency, 2005). Therefore, all information media used to inform citizens about possible hazards should be published online in accessible formats so everybody can access that important content.

Social networks

Social networks, similar to the Internet more generally, are another means for dissemination of information in a possible emergency. However, it is important that the veracity of the information be confirmed, without limiting social media. Best practice is for government entities to develop and have their own applications and information channels on the Internet and social networks, so that citizens can have confidence in the accuracy of information and the official nature of warning or alerts, as well as safety reminders and preparedness tips.

Social networks are quite flexible, messages can be short and spread quickly: for example, through Twitter, Facebook, Instagram, WhatsApp, etc. However, it is not possible to control the messages on social networks once they have been sent, and misinformation can spread. Thus, it is important, as noted above, that governments build their own applications to inform the people, as well as to develop the means to verify information reported via social media.

Amateur radio

Radio amateurs have supported communications in emergency situations on a voluntary basis since the beginning of radio communications. They are experts in radio communications and have the equipment, skills and necessary frequencies allocated by ITU (2017d) to deploy networks in emergency events quickly and efficiently. Amateur radio activity is authorized in accordance with the licenses issued by national governments: therefore, they are authorized to re-establish national and international communications if necessary.

To ensure that radio amateurs have the training and skills necessary to support communications in case of an emergency, the International Amateur Radio Union has developed a guide for emergency telecommunications that allows potential operators to be trained (International Amateur Radio Union, 2015).

Radio amateurs can help in a possible emergency with communications of different types: for example, supporting an international institution such as the International Federation of the Red Cross and Red Crescent Societies;[8] providing communications to those displaced by the disaster and/or other relief efforts; providing support to the emergency management agency of the national government by providing inter-institutional communications; or supporting logistics communications to the humanitarian agencies on the ground, e.g., firefighters or civil defence workers, among others.

[8] The International Federation of the Red Cross and the International Amateur Radio Union signed a Memorandum of Understanding on Cooperation in Emergency: Telecommunications for Disaster Preparedness and Response, which has been in place for more than a decade. Available at www.iaru.org/uploads/1/3/0/7/13073366/ifrcandiarumou.pdf (accessed 22 February 2019).

The support provided by radio amateurs in cases of emergency has the following advantages:

- There is great coverage, due to the large number of amateur radio stations available and operating in all regions and in almost every country in the world.
- The coverage of amateur radio stations becomes a network independent of others.
- There are training programmes and simulation exercises for emergencies developed by national radio amateurs for situations of telecommunications in emergencies.
- They are qualified temporary volunteers who provide skills and experience essential for emergency telecommunications, with the sole purpose of supporting humanitarian aid services.
- They have skill in solving problems related to the use of telecommunications during emergencies with often very limited resources.
- Many amateur radio stations trained to handle emergency telecommunications have alternative power sources, such as battery power, solar power or generator power and can operate during power disruptions.

The coverage of amateur radio networks can vary between short-range networks, *i.e.*, tens of kilometres, to long-range networks that exceed 500 km. Additionally, amateur radio satellites can be used for medium- and long-range communications, fulfilling the function of storage and retransmission.

It is important to mention that radio amateurs should only carry out or accept tasks that are foreseen in the agreements reached with other stakeholders, such as government authorities, that clarify their role in emergency operations. Volunteer radio amateurs typically do not make decisions in rescue operations and are usually only qualified or authorized to send and receive accurate communications. The normal role of the amateur radio service is to establish and support communications for those who directly carry out emergency operations.

Finally, it is also important to note that reliance on amateur radio networks can present certain disadvantages in countries without a robust and active amateur radio population due to an insufficient number of amateur radio operators. It is important for administrations in countries without an active amateur radio service to foster and promote the growth of amateur radio so as to provide an adequate supply of amateur radio operators is available during emergency telecommunications operations.

Broadcasting

One of the most powerful means of transmitting information to the general public is radio (voice) and TV broadcasting. Broadcasting is one of the mediums that has been in the public service the longest, with radio broadcasting dating back to the early twentieth century, and TV broadcasting in service since 1930. In this sense, radio and TV broadcasting services present one of the highest penetrations in terms of population.

For the specific case of emergencies and disasters, radio broadcasting plays a fundamental role in informing the public about the various situations that may arise, including breaking news alerts that can interrupt the usual programming. The government entities in charge of dealing with emergencies should be in continuous communication with the radio and television broadcasting stations when the situation warrants such communication. This ensures that the information that is transmitted to the public is as up to date and accurate as possible. In addition, the government should also facilitate access and help journalists who want to cover events in real time from the affected areas. In this sense, it is recommended to build meeting points for the press near areas of interest but far from high-risk zones.

Likewise, a warning system can be connected to broadcasting stations in such a way that they can interrupt the usual programming in case of emergency to transmit information to the public, such as evacuation orders.

Finally, as is the case for the infrastructure of other communications, for broadcasting it is important to:

- maintain reserve and alternative power generation systems;
- place transmission stations in areas of low risk in the event of disasters; and
- take into account the risks of the area and take appropriate measures (e.g., anti-seismic constructions) in the construction of transmission and programming stations and the links between them.

Annex E: Additional information on the Tampere Convention

The Tampere Convention, currently ratified by 49 countries, emerged out of an assembly of 225 delegates from 75 countries in the city of Tampere, Finland, in 1998, and entered into force on 8 January 2005.

This Convention is based on the following basic principles (International Federation of Red Cross and Red Crescent Societies, 2011):

- Reduce regulatory barriers: Signatories agree to reduce regulatory barriers to the transit of personnel, equipment, materials and information through the affected territory. Parties to the Convention agree to "reduce or eliminate regulatory barriers to the use of telecommunications resources for mitigation and disaster relief". The scope of the agreement includes restrictions on the mobility of essential personnel and imports/exports, as well as use of certain types of equipment, radio-frequency spectra, and licensing requirements and fees.
- Guarantee the necessary privileges, immunities and facilities for relief personnel and organizations providing telecommunication assistance: Signatories agree, as permitted by the national law of each country, to grant personnel and organizations involved in relief operations:
    - Immunity from arrest, detention or prosecution.
    - Immunity from confiscation or embargo of their equipment, materials and property.
    - Exemptions from tax obligations and other charges (excluding value added tax).
    - Access to local facilities.
    - Exemption from licensing requirements or fast tracking of licensing applications.
    - Protection of staff, equipment and materials.
- Respect for the sovereignty of the country receiving assistance: Recipient States maintain full control over the initiation and termination of the assistance, as well as the power to reject all or part of the assistance offered. Likewise, the recipient countries also maintain the right to direct, control, coordinate and supervise telecommunication assistance provided under the Convention within their territory.
- Improve coordination and exchange of information: The United Nations Emergency Relief Coordinator (supported by OCHA) is designated the "operational coordinator" by the Convention, with a number of tasks aimed at improving coordination and information sharing regarding telecommunication assistance. It is also determined that applications for telecommunication assistance can be made directly to the receiving country or through the operational coordinator. Furthermore, signatory countries should keep the operational coordinator informed of both the national authorities responsible for matters relevant to the Convention and the national authorities that can identify telecommunication resources available for use during disaster mitigation and response. Finally, in the Convention, the parties agree to share information on hazards and disasters between each other, non-State entities, intergovernmental organizations and the public.

Considering the above, ascension to an international treaty can require consultations or approvals of different legislative and executive bodies at the national level. It may also be necessary to adapt national laws and regulations to avoid conflict with particular articles of the treaty. Counties that have signed Tampere must have relevant procedures in place that enable the import of communications equipment. With this in mind, the following aspects may require special attention from a signatory country (ITU, 2006b):

- The Convention aims to accelerate and facilitate the use of emergency communications in the context of international humanitarian assistance. Communications aid can be directly provided

to national institutions, to a specific location affected by a catastrophe, and/or in support of other relief or risk management activities.

- The Convention provides for special privileges and the immunity from prosecution of governmental entities, international organizations, NGOs and other non-State entities.
- The Convention fully protects the interests of States requesting and receiving assistance. The beneficiary government retains the right to supervise all assistance provided.

Finally, the operation of the Convention is carried out by different non-governmental entities and intergovernmental organizations. In particular, "The Secretary-General of the United Nations is the custodian of the Convention (article 16). The Treaty Section of the Office of Legal Affairs of United Nations Headquarters, New York, is in charge of the relevant procedures. The United Nations Emergency Relief Coordinator is concerned with coordinating operations for the implementation of the Convention (article 2). The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) is responsible for the fulfilment and performance of the respective functions and works closely with the International Telecommunication Union (ITU). The Working Group on Telecommunications in Emergencies (WGET) is the advisory Board for the work." Source: ITU (2005).

Annex F: Additional information on drills and exercises

In general, four types of drills and simulations can be identified: table-top exercises (TTX), drills, functional exercises and full-scale exercises:

- Table-top exercises (TTX) refers to a facilitated discussion of a simulated emergency, generally conducted in a low-stress environment with participants seated around a table.
- A *drill* is an activity in which specific operations, functions or systems are repeatedly tested in a supervised setting. It calls for the mobilization and use of resources, such as a weekly radio check or a monthly fire drill, for example.
- Functional exercises are fully simulated interactive exercises that test the capability of an agency to respond to a simulated event. This type of exercise aims to test multiple functions of an emergency plan and deliver a more "real" experience than drills and/or table-top exercises.
- Finally, the full-scale exercise is designed to evaluate the operational capability of emergency management systems in a highly stressful environment, simulating actual response conditions. This type of exercise requires a large amount of resources and coordination, as it typically involves multiple agencies and participants physically deployed in a field location. Full-scale exercises aim to test almost all functions of an emergency plan.

Annex G: Additional information on ICT to support people with specific needs

Incorporation of multiple forms of ICT is key to bringing messages to all people, without discrimination of age, gender, ability or location. To ensure this inclusiveness, the following considerations are required:

- Public address systems: Alerts in audio and visual formats through public loudspeakers and electronic displays in public spaces such as railway platforms, consumer markets, parks and other public areas can reach people who may not have access to personal ICT devices. When possible, graphics and images should be displayed in addition to text. Sirens can be accompanied by flashing lights to denote the nature and level of threat.
- Radios: Radios can be used with attachments or with special features to enable use by people who are deaf or hard of hearing. For example, devices such as the special-needs National Oceanic and Atmospheric Administration weather radio in the United States of America can transmit broadcasts as vibrations, flashing lights and simple texts to alert individuals who are deaf and hard of hearing of weather and disaster warnings.
- Television: Employing closed captioning or subtitling in local languages can make audio commentary accessible to people who have hearing impairments or do not understand the language. In addition, sign language interpreters should be used when providing televised information about a disaster or emergency situation.
- SMS: If information is sent out only as SMS, people who need non-visual inputs and don't have access to high-end devices that can convert text to other formats such as audio will be excluded. Hence, warnings and alerts should also go out in multiple formats across different dissemination channels.
- E-mail: Notifications should be enabled in multiple languages. The software should be designed as per accessibility guidelines to enable it to operate seamlessly with a user's assistive technology. Some desktop alerting systems can ensure that pop-up messages are delivered in different formats in addition to just texts and audio beeps. For example, the company Desktop Alert, Inc. has developed a product that reads out an entire emergency alert message, making it accessible to people who have visual disabilities, as well as those who may be stationed at a distance from their computers. Use of graphics within the alert may assist people who have trouble understanding the language, children and individuals with cognitive disabilities.
- Social networks: Social media sites should also be designed to be accessible and to work with a user's assistive technology. Alternative social media sites attempt to fill the gap when traditional media may not be fully accessible. For example, Easy Chirp20 offers an alternative web-based interface to Twitter to enable accessibility for persons with disabilities, as well as to provide access to people using low bandwidths, without Java Script, and those on older browsers. The Emergency 2.0 Wiki Accessibility Toolkit21 offers education and information to persons with disabilities on using social media at different stages of a disaster or emergency, and also lists apps and social media available for use. Finally, although the new versions of the most popular social networks are offering accessibility features, it is important that the agencies publishing emergency information on these platforms know about electronic content accessibility to ensure that the messages are accessible.
- Websites: Websites providing disaster management information must be tested for accessibility to ensure that persons with disabilities do not face barriers in accessing the important information shared on the website. Fact sheets, handbooks and manuals may be unusable by persons using screen readers if they are in formats that cannot be read aloud, such as JPEG files or inaccessible image-based PDFs. On the other hand, images and graphics are excellent ways to depict content for children, people with cognitive disabilities, or people with linguistic differences; however, these must be supplemented with textual information to ensure that persons with visual impairments are able to understand the information.

Finally, other types of technologies, such as Geographical Information System (GIS), can also be useful to help people with special needs during an emergency. This computer system, which allows users to store, analyse and manipulate different types of data according to their geographical attributes and provide real-time spatial information, can be an effective tool for providing geographic information to potentially vulnerable areas. For example, information from a disabled person registry can be used in conjunction with weather, natural conditions and available disaster-response infrastructure to calculate risks and hazards, both in advance and in real time during disasters. Likewise, GIS can be used to understand the possible vulnerabilities of different groups of the population and develop specific efforts during mitigation, preparedness, response and recovery. GIS modelling can also help simulate evacuations and plan safe evacuation routes that are essential for people with reduced mobility, which can be vital in situations where, for example, previously designated evacuation routes are blocked (e.g., because of a landslide, accumulation of debris or collapse of buildings) (ITU, 2017a; 2017c).

References

Akhtaruz, Z. and A.K.M. Abdul (2017). Application of ICT Tools for Climate Change and Disaster Management in Bangladesh.

Christian, E. (2016). Survey of Other Common Alerting Protocol (CAP) Implementations. 24 August. Bangkok.

Centre for Research on the Epidemiology of Disasters (CRED) (2017). Annual Disaster Statistical Review 2016. Brussels. Available at emdat.be/sites/default/files/adsr_2016.pdf (accessed 23 February 2019).

Farnham, J.W. (2005). Disaster and emergency communications prior to computers/Internet: a review. *Critical Care*, vol. 10 (14 December), p. 207.

Global Facility for Disaster Reduction and Recovery (2013). Post-Disaster Needs Assessments – Volume A: Guidelines. European Commission, United Nations Development Group and World Bank.

International Amateur Radio Union (2015). Emergency Telecommunications Guide. 16 March.

International Federation of Red Cross and Red Crescent Societies (2011). Background Information Sheet – Tampere Convention: Core Provisions and Benefits. Geneva, March.

(2012). Contingency planning guide. Geneva.

International Telecommunication Union (ITU) (N.D.). Uganda: Harnessing the power of ICTs to promote disaster risk reduction. Available at www.itu.int/en/ITU-D/Pages/MakeADifference/How-we-make-a-difference-Uganda.aspx (accessed 22 February 2019).

(2001). Handbook on disaster communications. Geneva, 20 June.

(2006a). Emergency and Disaster Relief. Geneva.

(2006b). Handbook on Emergency Telecommunications Edition 2005. Geneva, 3 March.

(2007a). Compendium of ITU's work on Emergency Telecommunications. Geneva, 24 September.

(2007b). Standard X.1303. Geneva. Available at www.itu.int/rec/T-REC-X.1303 (accessed 24 February 2019).

(2010). Radiocommunication RS.1859. Use of remote sensing systems for data collections to be used in the event of natural disasters and similar emergencies. Geneva.

(2012). Basic Principles for a National Emergency Communications Plan. Bogota, 24–26 July.

(2013). Technical Report on Telecommunications and Disaster Mitigation. Telecommunication Standardization Sector of ITU. Geneva.

(2017a). Accessible ICTs for persons with disabilities: Addressing preparedness. Centre for Internet and Society (CIS) (India). 31 January.

(2017b). ICT Facts and Figures. Geneva. Available at www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx (accessed 24 February 2019).

(2017c). Question 5/2**:** Utilization of telecommunications/ICTs for disaster preparedness, mitigation and response. Geneva. Available at www.itu.int/pub/D-STG-SG02.05.1-2017 (accessed 24 February 2019).

(2017d). Radiocommunication M.1732-2. Characteristics of systems operating in the amateur and amateur-satellite services for use in sharing studies.

(2017e). Radiocommunication BT.2299-2. Broadcasting for public warning, disaster mitigation and relief.

Japan Times (2012). Deaf in Tohoku get free video help. Available at www.japantimes.co.jp/news/2012/03/16/national/deaf-in-tohoku-get-free-video-help/#.W8ezHGhKiM8). (accessed 22 February 2019).

Ministry of Transport and Telecommunications of Chile, Decree 125 of 2013.

Ministry of Transportation and Communications of Peru (2007). Decree 030-2007. Available at http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_1280.pdf (accessed 21 February 2019).

National Council on Disability (2014). Effective Communications for People with Disabilities: Before, During, and After Emergencies. Washington, D.C., 27 May.

NetHope (2018). Planning a disaster: Detail and expertise required for disaster preparation training. Available at https://nethope.org/2018/07/17/planning-a-disaster-detail-and-expertise-required-for-disaster-preparation-training/ (accessed 22 February 2019).

Qureshi, A. (2012). Accessible ICT tools and services in disaster and emergency preparation. Global Alliance on Accessible Technologies and Environments.

SAFECOM and NCSWIC (2019), Emergency Communications Governance Guide for State, Local, Tribal, and

Territorial Officials.

Tampere Convention (1998). Available at www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf (accessed 25 February 2019).

United Kingdom (2010). National Emergency Plan for the Telecommunications Sector.

United Nations (2016). *Report of the Open-ended Intergovernmental Expert Working Groupon Indicators and Terminology Related to Disaster Risk Reduction (OIEWG)* (A/71/644), adopted by the General Assembly on 2 February 2017 (A/RES/71/276)

(2015a). Sendai Framework for disaster risk reduction 2015–2030. Available from www.unisdr.org/we/coordinate/sendai-framework (accessed 25 February 2019).

(2015b). Transforming our World: The 2030 Agenda for Sustainable Development. Available at https://sustainabledevelopment.un.org/post2015/transformingourworld (accessed 25 February 2019).

United Nations International Strategy for Disaster Reduction (UNISDR) (2018). Implementation guide for local disaster risk reduction and resilience strategies – A companion for implementing the Sendai Framework target E. Geneva.

(2006a). Global Survey of Early Warning Systems. Geneva

(2006b). Developing Early Warning Systems: A checklist. Geneva

United States Department of Homeland Security (N.D.). SAFECOM, Writing Guide for Standard Operating Procedures. Available atwww.dhs.gov/sites/default/files/publications/Writing%20Guide%20for%20Standard%20Operating%20Procedures_0.pdf (accessed 21 February 2019).

(2013). Innovative Uses of Social Media in Emergency Management. Washington, D.C.

(2014). National Emergency Communications Plan. Washington, D.C.

(2016). Land Mobile Radio (LMR) 101. Washington, D.C.

United States Federal Emergency Management Agency (2005). Effective Communication.

World Bank (2016). Learning from disaster simulation drills in Japan.

World Health Organization (2011). Disaster Risk Management for Health: People with disabilities and older people.

World Meteorological Organization (2018). Multi-hazard Early Warning Systems: A Checklist.

List of ITU-T documents related to emergency telecommunications

- Recommendation ITU-T E.106 "International Emergency Preference Scheme for disaster relief operations (IEPS)"
- Recommendation ITU-T E.107 "Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS"
- Recommendation ITU-T E.108 "Requirement for Disaster Relief Mobile Message Service"
- Recommendation ITU-T E.119 "Requirements for safety confirmation and broadcast message service for disaster relief"
- Recommendation ITU-T E.123 Amendment 1 "Notation for national and international telephone numbers, e-mail addresses and Web addresses: Contact information in case of emergency for mobile telephones"
- Recommendation ITU-T E.161.1 "Guidelines to select Emergency Number for public telecommunications networks"
- Recommendation ITU-T E.164 Supplement 5 “Guidance with regard to the selection of numbers for helplines for children”
- Recommendation ITU-T H.246 Amendment 1 "Mapping of user priority level and country/international network of call origination between H.225 and ISUP"
- Recommendation ITU-T H.248.44 "Gateway control protocol: Multi-Level precedence and pre-emption package"

- Recommendation ITU-T H.248.81 "Gateway Control Protocol: Guidelines on the Use of the international emergency preference scheme (IEPS) call indicator and priority indicator in ITU-T H.248 Profiles", including Amd.2 (2015) with support for DiffServ signaling
- Recommendation ITU-T H.323 Annex M5 for transport of common alerting protocol (CAP) messages in ITU-T H.323 systems
- Recommendation ITU-T H.460.4 "Call priority designation and country/international network of call origination identification for H.323 priority calls"
- Recommendation ITU-T H.460.14 "Support for Multi-Level Precedence and Preemption (MLPP) within H.323 Systems"
- Recommendation ITU-T H.460.21 "Message broadcast for H.323 systems"
- Recommendation ITU-T H.785.0 "Digital signage: Requirements of disaster information services"
- Recommendation ITU-T J.260 "Requirements for Emergency/Disaster Communications over IPCablecom Networks"
- Recommendation ITU-T J.261 "Framework for implementing preferential telecommunications in IPCablecom and IPCablecom2 networks"
- Recommendation ITU-T J.262 "Specifications for authentication in preferential telecommunications over IPCablecom2 networks"
- Recommendation ITU-T J.263 "Specification for priority in preferential telecommunications over IPCablecom2 networks"
- Recommendation ITU-T L.390 "Disaster management for outside plant facilities"
- Recommendation ITU-T L.392 "Disaster management for improving network resilience and recovery with movable and deployable ICT resource units"
- Recommendation ITU-T M.3350 "TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)"
- Recommendation ITU-T P.1140 "Speech communication requirements for emergency calls originating from vehicles"
- Signalling for IEPS support in ISUP: ITU-T Q.761 Amd.3, ITU-T Q.762 Amd.3, ITU-T Q.763 Amd.4, and ITU-T Q.764 Amd.4
- Signalling for IEPS support in BICC: ITU-T Q.1902.1 Amd.2, ITU-T Q.1902.2 Amd.3, Q.1902.3 Amd.3, and Q.1902.4 Amd.3
- Signalling for IEPS support in CBC: ITU-T Q.1950 Amd.1 Annex G
- Signalling for IEPS support in ATM AAL2: ITU-T Q.2630.3 Amd.1
- Signalling for IEPS support in B-ISUP: ITU-T Q.2762 Amd.1, Q.2763 Amd.1 and Q.2764 Amd.1
- Signalling for IEPS support in DSS2: ITU-T Q.2931 Amd.5
- Recommendation ITU-T X.1303 "Common Alerting Protocol (CAP V1.1)"
- Recommendation ITU-T X.1303 bis "Common Alerting Protocol (CAP V1.2)"
- Recommendation ITU-T Y.2074 "Requirements for Internet of Things devices and operation of Internet of Things applications during disaster"
- Recommendation ITU-T Y.1271 "Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packet-switched networks"
- Recommendation ITU-T Y.2171 “Admission control priority levels in Next Generation Networks”
- Recommendation ITU-T Y.2172 “Service restoration priority levels in Next Generation Networks”

- Recommendation ITU-T Y.2205 "Next Generation Networks- Emergency Telecommunications – Technical Considerations"
- Recommendation ITU-T Y.2222 | Y.4250 "Sensor control networks and related applications in a next generation network environment"
- Recommendation ITU-T Y.2705 "Minimum security requirements for interconnection of emergency telecommunications service (ETS)"
- Recommendation ITU-T Y.4119 "Requirements and capability framework for IoT-based automotive emergency response system"

Non-normative publications:

- Supplement 1 to ITU-T E.100 series Recommendations "Framework of disaster management for disaster relief system"
- Supplement 5 to Recommendation ITU-T E.164 "Guidance with regard to the selection of numbers for helplines for children"
- Supplement 9 to ITU-T H-Series Recommendations, "Gateway Control Protocol: Operation of H.248 with H.225.0, SIP, and ISUP in Support of Emergency Telecommunications Service (ETS)/ International Emergency"
- Supplement 12 to ITU-T H-series Recommendations "Gateway control protocol: Priority traffic treatment by ITU-T H.248 gateways"
- Supplement 35 for ITU-T L-series Recommendations "Framework of disaster management for network resilience and recovery"
- Supplement 47 to ITU-T Q-series Recommendations, "Emergency services for IMT-2000 networks – Requirements for harmonization and convergence"
- Supplement 53 to ITU-T Q-series Recommendations "Signalling requirements to support the International Emergency Preferential Scheme (IEPS)"
- Supplement 57 to ITU-T Q-series Recommendations "Signalling Requirements to support the Emergency Telecommunication Service (ETS) in IP Networks"
- Supplement 61to ITU-T Q-series Recommendation "Evaluation of signalling protocols to support Y.2171 admission control priority levels"
- Supplement 62 to ITU-T Q-series Recommendations "Overview of the work of standards development organizations and other organizations on emergency telecommunications service". A revision of this document was approved by ITU-T SG 11 in February 2014.
- Supplement 63 to ITU-T Q-series Recommendations "Signalling protocol mappings in support of the Emergency Telecommunications Service in IP networks" approved by ITU-T SG 11 in June 2013.
- Supplement 68 to ITU-T Q-series Recommendations "Emergency Telecommunications Service (ETS) interoperability limitations" approved by ITU-T SG 11 in December 2015.
- Supplement 69 to ITU-T Q-series Recommendations "Framework for interconnection between VoLTE-based network and other networks supporting emergency telecommunications service (ETS)"
- Supplement 19 to ITU-T Y-series Recommendations "Risk analysis service over Next Generation Network"
- Publication in three parts on using submarine cables for climate monitoring and disaster warning (2012): "Opportunities and legal challenges", "Strategy and roadmap" and "Engineering Feasibility Study"
- Technical Paper HSTP-DIS-UAV (2018) "Use cases and service scenarios of disaster information service using unmanned aerial vehicles"

Abbreviations

CAP	Common Alerting Protocol
CRED	Centre for Research on the Epidemiology of Disasters
CRPD	United Nations Convention on the Rights of Persons with Disabilities
ETC	Emergency Telecommunications Cluster
EWS	Early Warning System
FEMA	Federal Emergency Management Agency (United States of America)
FSS	Fixed Satellite Service
GIS	Geographical Information System
GPS	Global Positioning System
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union Development Sector
ITU-R	International Telecommunication Union Radiocommunication Sector
LMR	Land Mobile Radiocommunications
MSS	Mobile Satellite Service
MTC	Ministry of Transportation and Communications (Peru)
NDMO	National Disaster Management Organization
NETP	National Emergency Telecommunication Plan
NGO	Non-Governmental Organization
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
RBS	Radio Base Station
SMS	Short Message Service
SOP	Standard Operating Procedures
	Telecommunication and Information and Communication Technology
TTX	Table-top exercises
UN	United Nations
UNDRR	United Nations Office for Disaster Risk Reduction
VSAT	Very Small Aperture Terminal
WFP	World Food Programme
WLL	Wireless Local Loop

Glossary[1]

Contingency Planning: A management process that analyses disaster risks and establishes arrangements in advance to enable timely, effective and appropriate responses.

Critical infrastructure: The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society.

Disaster: A serious disruption of the functioning of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability and capacity, leading to one or more of the following: human, material, economic and environmental losses and impacts.

Disaster Management: The organization, planning and application of measures preparing for, responding to and recovering from disasters.

Disaster Risk: The potential loss of life, injury, or destroyed or damaged assets which could occur to a system, society or a community in a specific period of time, determined probabilistically as a function of hazard, exposure, vulnerability and capacity.

Disaster Risk Management: A qualitative or quantitative approach to determine the nature and extent of disaster risk by analysing potential hazards and evaluating existing conditions of exposure and vulnerability that together could harm people, property, services, livelihoods and the environment on which they depend.

Early Warning System: An integrated system of hazard monitoring, forecasting and prediction, disaster risk assessment, communication and preparedness activities systems and processes that enables individuals, communities, governments, businesses and others to take timely action to reduce disaster risks in advance of hazardous events.

Economic loss: Total economic impact that consists of direct economic loss and indirect economic loss. Direct economic loss is the monetary value of total or partial destruction of physical assets existing in the affected area. Indirect economic loss is a decline in economic value added as a consequence of direct economic loss and/or human and environmental impacts.

Evacuation: Moving people and assets temporarily to safer places before, during or after the occurrence of a hazardous event in order to protect them.

Exposure: The situation of people, infrastructure, housing, production capacities and other tangible human assets located in hazard-prone areas.

Hazard: A process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation.

Mitigation: The lessening or minimizing of the adverse impacts of a hazardous event.

Preparedness: The knowledge and capacities developed by governments, response and recovery organizations, communities and individuals to effectively anticipate, respond to and recover from the impacts of likely, imminent or current disasters.

Prevention: Activities and measures to avoid existing and new disaster risks.

Recovery: The restoring or improving of livelihoods and health, as well as economic, physical, social, cultural and environmental assets, systems and activities, of a disaster-affected community or society, aligning with the principles of sustainable development and “build back better”, to avoid or reduce future disaster risk.

[1] https://www.unisdr.org/we/inform/terminology#letter-h

Resilience: The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management.

Response: Actions taken directly before, during or immediately after a disaster in order to save lives, reduce health impacts, ensure public safety and meet the basic subsistence needs of the people affected.

Vulnerability: The conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards.

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)
Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)
Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)
Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: ituteguciglapa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt
International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand
International Telecommunication Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU) Area Office
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland
International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-31321-0

Published in Switzerland
Geneva, 2020