

GLOBAL GUIDELINES TO DEVELOP NATIONAL  
EMERGENCY TELECOMMUNICATION PLANS

# DRAFT FOR COMMENTS

March 2019

**Deadline for comments: 30 April 2019**





Please send all comments to:

Maritza Delgado

[delgadod@itu.int](mailto:delgadod@itu.int)

# Global Guidelines to Develop National Emergency Telecommunication Plans

## Contents

Acknowledgements.....	4
Abbreviations .....	5
Executive summary .....	6
1. Document overview .....	12
1.1. Purpose .....	12
1.2. Target audience.....	12
1.3. What is an NETP? .....	12
1.4. Benefits of an NETP .....	13
1.5. Scope and overall structure of the document .....	14
2. Introduction .....	14
3. Typology of disasters.....	15
3.1.  Climatological disasters.....	16
3.2.  Geophysical disasters .....	17
3.3.  Hydrological disasters.....	17
3.4.  Meteorological disasters .....	18
3.5. Technological disasters .....	18
3.6. Historical disasters by region .....	18
3.6.1. Africa .....	21
3.6.2. Americas.....	21
3.6.3. Arab States .....	21
3.6.4. Asia–Pacific.....	22

3.6.5.	Commonwealth of Independent States .....	22
3.6.6.	Europe .....	22
4.	Phases of disaster management .....	26
4.1.	Disaster mitigation .....	26
4.2.	Preparedness.....	27
4.3.	Response and recovery .....	28
4.4.	Principles for the development of an NETP .....	29
5.	International cooperation and coordination .....	30
5.1.	Emergency Telecommunications Cluster .....	30
5.2.	International Telecommunication Union .....	31
5.3.	Tampere Convention.....	32
5.4.	United Nations Office for the Coordination of Humanitarian Affairs .....	35
5.5.	United Nations International Strategy for Disaster Reduction .....	36
5.6.	Bilateral agreements .....	37
6.	National disaster management .....	37
6.1.	Legal and regulatory framework .....	38
6.2.	Administrative structure and governance model .....	41
6.3.	Public–private cooperation, coordination, communication and contingency plans .....	45
6.4.	Communication channels.....	46
6.5.	Contingency plans .....	47
6.6.	Definition of roles and identification of contact points .....	47
7.	Telecom/ICT legislation and regulation .....	48
7.1.	Legislation .....	49
7.2.	Regulation .....	49
8.	Telecom/ICTs for emergencies.....	53
8.1.	Telecom/ICT services.....	54
8.1.1.	Public telecom/ICT services.....	54
8.1.2.	Private telecom/ICT services .....	60
8.1.3.	Internet.....	62
8.1.4.	Social networks .....	63
8.1.5.	Amateur radio .....	63

8.1.6. Broadcasting.....	65
8.2. Vulnerability and risk analysis of telecom/ICT networks .....	65
8.2.1. Telecom/ICT database for emergencies.....	66
8.3. Early Warning Systems .....	66
8.4. Common Alerting Protocol.....	68
9. Development of capacities and drills .....	71
9.1. Drills and simulations in practice .....	73
10. Support for people with specific needs .....	77
10.1. Telecom/ICT to support people with specific needs during emergency events.....	78
11. NETP: Step by step .....	82
11.1. Topics to be included in the NETP.....	82
11.2. Drafting the NETP .....	83
11.2.1. General introduction .....	83
11.2.2. Mitigation phase .....	84
11.2.3. Preparedness phase .....	84
11.2.4. Response phase.....	85
11.2.5. Recovery phase .....	86
11.3. NETP drafting process .....	87
Annex A – Emergency communications checklist.....	89
References.....	99

## Acknowledgements

The present Global Guidelines were prepared by International Telecommunication Union (ITU) expert Juan Manuel Roldan, President of Luxon Consulting Group, LLC, and research assistant Felipe Ordoñez, under the direction of the Least Developed Countries, Small Island Developing States and Emergency Telecommunication Division (LSE), within the Projects and Knowledge Management Department of ITU's Telecommunication Development Bureau. Cyril Brunet contributed to the graphic design.

ITU would like to express its appreciation to Don Wallance and Mathew Lloyd for their useful inputs and comments.

## Abbreviations

CAP	Common Alerting Protocol
CRED	Center 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-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
telecom/ICT	telecommunication and information and communication technology
TTX	tabletop exercises
UN	United Nations
UNISDR	United Nations International Strategy for Disaster Reduction
VSAT	Very Small Aperture Terminal
WFP	World Food Programme
WLL	wireless local loop

## Executive summary

This document aims to assist national authorities and policy-makers in the development of National Emergency Telecommunication Plans (NETPs). It offers a clear, flexible and user-friendly framework that advises countries on how to develop strategies for the effective and efficient use of information and communication technologies (ICTs), and telecommunication and ICT (telecom/ICT) networks and services for early warning and during emergencies.

An NETP is a strategic plan to best manage the risk of disasters during the mitigation, preparedness, response and recovery phases, by promoting communication and information sharing across all levels of government, within communities at risk, and between public and private organizations. The development of an NETP must include key elements and concepts, such as the types of hazards that might occur, the phases of disaster management and how telecommunication networks and services and ICTs can provide support. It will cover legislation and policies for disaster risk management, and the international framework for cooperation in emergencies.

While developing an NETP, it is important to consider the disaster risk profile of the specific region, as well as the most frequent and deadly emergency events that have occurred in the past. There are different types of disasters – such as climatological, geophysical, hydrological, meteorological or technological – that can cause serious damage to the population and generate substantial economic losses.

The gradual increase in global temperatures has been linked to the intensity of climate-related disasters. The past 4 years (2014–2018) have been the hottest on record, and the 20 warmest have occurred in the past 22 years. In only the last ten years (2008–2017), disaster events have affected 2 billion people globally, causing almost USD 1.8 trillion (in 2017 dollars) in economic damage, and more than 722 000 fatalities. It is essential that an NETP take into account the likely types of future disasters and potentially affected locations.

Distinct types of disasters can affect countries and regions in very different ways. For example, a riverside area may be more likely to face hydrological-type disasters, while a region in the vicinity of volcanoes would be more likely to face geophysical-type disasters. Consequently, an NETP should consider identifying appropriate telecom/ICT risk management measures in each location within a country's territory, including, for example, different warning system requirements or specific assessments of critical infrastructure in each particular region. For that reason, the NETP must develop and include geographic maps of strategic locations based on the specific risks they may face.

**Recommendation 1:** Geographic maps depicting the likely locations of possible disasters should be developed and included in the NETP. This is critical for the analysis of telecom/ICT infrastructure risks and contingency plans, as well as for determining the type of warning systems needed.

A well-conceived NETP should also incorporate the four phases of disaster management: mitigation, preparedness, response and recovery. The mitigation phase includes aspects such as education and awareness of existing risks; vulnerability assessments; and the construction or maintenance of necessary infrastructure, including telecom/ICT, to make the community more resilient and lessen the potential impact of future disasters. The preparedness phase considers the establishment of a NETP, drills, Early Warning Systems (EWSs) and operational processes. The response and recovery phases refer to aspects of coordination and communication, as well as the restoration of infrastructure and services during and after a disaster.

**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 telecom/ICT will be helpful in each of these phases. In addition, the development and implementation of the NETP should be governed by the following principles:

- Adopt a strategy that addresses all potential hazards to which the nation is exposed.
- Obtain commitments to participate, contributions and agreement on a strategy from all stakeholders.
- Ensure the NETP addresses the links between different phases of disaster management in different types of disasters.
- The NETP should include training, drills and evaluation of telecom/ICT infrastructure to be used in all phases of disaster management and at all levels – individual, team, department and community.
- During NETP implementation, decisions must be based upon accurate assumptions about all potential disaster types.
- Standard operating procedures should identify the types of communications/technologies that are required for a given type of emergency.

A well-developed NETP should also take into account the different mechanisms available for international cooperation for disaster risk management. The Emergency Telecommunications Cluster (ETC), ITU, the United Nations International Strategy for Disaster Reduction (UNISDR), or the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), among others, can provide global assistance and guidelines for disaster risk management in all its phases. Also, in particular for telecom/ICT disaster management, the Tampere Convention is a treaty that provides a legal framework for using telecommunications within the scope of international humanitarian assistance. This framework reduces regulatory barriers and gives protections to personnel providing telecommunication support abroad, while respecting the national interests of the country receiving assistance.



In general, all frameworks and treaties that a country might sign, including bilateral or multilateral agreements, should be incorporated into national legislation in order to achieve maximum benefit from their provisions. In addition, the different agencies and people involved in the disaster risk management process in the country should be aware of them in order to execute them properly. This is of particular importance for the Tampere Convention to be successfully implemented.

**Recommendation 3:** The NETP should include a description 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 adhere to the Tampere Convention and to take the necessary actions at national and local level to ensure that the Convention will be effective in a disaster situation.

The development of an NETP should also be based on the existing national disaster risk management plan, which provides an institutional and inter-institutional framework for the actions of the government and civil society in the face of a threat or disaster. Furthermore, a national disaster risk management plan must define the methodologies and chain of command that will guide all stakeholders from different governmental and non-governmental organizations (NGOs) in the event of an emergency.

In that sense, an NETP should have a well-defined administrative structure involving all stakeholders, both national and international, within the territory where the emergency is likely to occur or has already occurred. Likewise, it must have a clear model of governance that allows for planning for, execution of and subsequent revision to the disaster response activities to be carried out. The disaster management process must take place under the leadership of the national government, which should define the responsibilities and procedures for all stakeholders at various levels acting in the face of a catastrophe.

**Recommendation 4:** 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 the national disaster risk management plan.

The development and implementation of an NETP also require a specific set of policies and legislation on emergency telecom/ICT that support the implementation of a comprehensive national approach. An NETP should support response at all levels during an emergency, and describe

how telecom/ICT will be managed in support of national disaster relief efforts, to ensure an effective response to a disaster event. Also, regulatory authorities and governments must have the mandate to issue adequate rules and regulations to implement those national laws. Such rules and regulations must describe in detail the responsibilities, protocols and strategies each stakeholder – including telecom/ICT operators, public and private organizations, government and local communities – must implement to effectively and efficiently assist in maintaining emergency telecom/ICT services during national disasters. In particular, the regulation should include aspects such as licensing, frequency allocation, priority call routing, network redundancy, type approval of ICT/telecom equipment, and importation of ICT/telecom equipment.

**Recommendation 5:** Legislation and regulation regarding telecom/ICT for disaster management should be in place and described in the NETP. Such legislation must provide general high-level guidance on the development of the NETP, while still allowing flexibility during its construction and implementation.

Telecom/ICT regulation regarding temporary licensing, type approval, import/export of equipment, frequency allocation, network redundancy and priority call routing, among others, should be enacted and enforced.

A description of both the legislation and regulation on telecom/ICT for disaster management must be included in the NETP.

Telecom/ICT facilities are essential to the management of operations before, during and after emergency and disaster events. The speed and effectiveness of emergency response depends on the speedy availability of information. In this sense, telecom/ICT services must be reliable and available when and where they are necessary. This can include the rapid deployment of temporary services in priority areas in the wake of a disaster. In order to support the availability of telecom/ICT services, the government should maintain an updated map of existing deployment of telecom/ICT infrastructure that includes the risks and vulnerabilities of telecom/ICT networks. For this purpose, it is essential that the NETP provides for regular maintenance of an updated database on the networks of the different telecom/ICT services. These services include public services via fixed and mobile networks; satellites; private services, such as land mobile radiocommunication (LMR) services and maritime, aeronautical and positional services; Internet and social networks; amateur radio; and broadcasting.

**Recommendation 6:** The NETP should contain information on all existing telecom/ICT networks (public and private), a vulnerability and risk analysis of all telecom/ICT networks, and network contingency plans for when emergencies and disasters occur. This information should be periodically reviewed and updated.

Along with the above, an NETP should also include an up-to-date inventory of the EWSs deployed in the national territory. These systems should, ideally, be linked with other hazard-based systems in the country in order to establish an integrated and efficient EWS network that considers not only the different potential disasters that might occur, but also the distinct needs that the end users may have.

**Recommendation 7:** Early Warning Systems should be designed and deployed, linking all hazard-based systems when possible to take advantage of economies of scale and enhance sustainability and efficiency through a multipurpose framework that considers multiple potential hazards and end-user needs. An inventory of such systems should be included in the NETP and periodically reviewed and updated.

Another important element to include in an effective NETP in order to prepare for emergency situations is a practical strategy for enhancing training and capacity building for both the administrators leading emergency responses and the wider community. Such capacity building requires not only practice drills, training activities, tests and other exercises, but also the development of a curriculum for these activities and the evaluation and possible modification of existing procedures and policies in light of limitations identified during capacity-building activities.

**Recommendation 8:** The NETP must include a mechanism for enhancing training and capacity building for both the administrators leading emergency responses and the wider community using telecom/ICT. 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 existing procedures and policies.

Finally, an adequate strategy for supporting people with specific needs should also be considered for all phases of disaster risk management. Considering the variety of difficulties people with specific needs could face during a disaster, the use of several different types of telecom/ICT can be vital to supporting these citizens before, during and after emergencies. Indeed, the use of multiple forms

of telecom/ICT in the dissemination of critical information is key to bringing messages to marginalized communities. Consequently, the strategies for preparing and responding to emergencies should include all available types of telecom/ICT and take into account the variety of possible needs of the general population.

**Recommendation 9:** The NETP should include multiple forms of telecom/ICT for the dissemination of warning alerts, which are key to bringing messages to all the people, including those with specific needs, and marginalized communities. It is important to ensure that the NETP understands and responds to everyone's needs.

This document ends with a chapter that addresses step by step how to build an NETP based on the information provided in these Global Guidelines.

Finally, it is important to highlight that the NETP must be periodically reviewed and updated after every drill and operation to incorporate lessons learned, or at least every three years if no drill and operation occur.

## 1. Document overview

### 1.1. Purpose

The purpose of this document is to assist national authorities and policy-makers in the development of National Emergency Telecommunication Plans (NETPs), based on their own needs and in their national visions for the optimal use of ICTs, and telecom/ICT for disaster management. This guide proposes a clear, flexible and user-friendly framework, which aims to advise countries on how to build a strategy for an effective and efficient use of telecom/ICT during emergencies.

The present document 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 with the aim of serving as a useful resource for stakeholders, by providing them with a framework that gradually guides the construction of the plan, based on recommendations and concepts from ITU, as well as from other global and representative experts and organizations.

An effective implementation of the NETP provides a methodical way to engage stakeholders in thinking through the life cycle of a potential disaster, determine required capabilities for emergency response, and establish a governance framework for roles and responsibilities. It also clarifies how to shape emergency planning and response; envisions and shares desired outcomes, and outlines effective ways to achieve them; and communicates expected results. The NETP must reflect what diverse stakeholder communities will need to focus on in order to address specific risks with the available resources they have or can obtain, based on the national disaster risk management plan.

### 1.2. Target audience

This guide is intended primarily for national authorities responsible for the development and implementation of NETPs in their respective countries. However, it is also a resource that can be useful for any person or organization generally involved in disaster risk management or in the administration of telecommunications during emergencies. This includes governments, the private sector, non-governmental entities, humanitarian aid agencies and private citizens, among others.

### 1.3. What is an NETP?

An NETP is a strategic plan that promotes communication and information sharing about threats, hazards and how to respond to them across all levels of government, within communities, and between public and private organizations. The creation of an NETP also entails defining policies, organizational structure and methods to be used in all phases of an emergency: i.e. mitigation, preparedness, response and recovery.

The NETP must adhere to the principles and objectives of each country's national disaster risk management plan. The NETP must also establish principles that guide the allocation of resources and responsibilities for the achievement of the proposed objectives, including expected telecom/ICT response times, tasks and processes.

#### 1.4. Benefits of an NETP

The effective management of disasters depends on the timely and effective delivery of information to those who need it in as close to real time as possible. In particular, timely information flow is important for early warning and alerting the population about disasters, enhancing the preparation for an emergency event, and for the effective coordination and articulation of response activities that can minimize economic losses, mitigate negative impacts to public well-being and, above all, reduce human fatalities caused by disasters.

The types of telecom/ICT that should be used throughout the entire cycle of disaster management include: initial detection of the disaster; public alerts and awareness; damage assessments; establishment of shelter locations; supply chain logistics and coordination; emergency medical support, including public health messaging post-disaster; determination of population safety and well-being; and search and rescue, among others (ITU, 2017c). This vital information must flow between various stakeholders, including citizens, government and public security officials, relief workers, private sector organizations and others (ibid.). Due to the critical role information flow plays in effective disaster response, telecom/ICTs are essential tools for conducting adequate disaster management. NETPs should be based on four principles: multihazard, multitechnology, multiphase and multistakeholder.

**Figure 1: Multistakeholder approach**



Considering the above, and taking into account the complex nature of emergency disaster response, it is important to develop clear guidelines for maintaining the flow of information. These guidelines are generally set out in the NETP. Ultimately, an NETP is a fundamental tool that helps reduce the negative impact on the population of an emergency event. In the last ten years, this impact has been

significant, with 2 billion people affected, almost USD 1.8 trillion (in 2017 dollars) in economic damage, and more than 700 000 fatalities around the globe.<sup>1</sup>

### 1.5. Scope and overall structure of the document

The objective of this document is to present a guide for any country, regardless of its particular risk exposure, to develop its own NETP. These guidelines are not intended to be an instruction manual that describes in detail how to establish a custom-made plan for each country. Instead, it serves as a general tool, on which any country around the globe can rely to develop its own NETP that fits the characteristics, needs and vulnerabilities of its specific territory.

Chapter 2 introduces the document, while Chapter 3 briefly describes each type of disaster and establishes a general profile of the hazards that are most common for each continent. Chapter 4 labels the phases of disaster management in order to incorporate them into the development of an NETP. Chapter 5 outlines existing international cooperation and coordination mechanisms, as well as how they can be implemented by a given country. Chapter 6 describes the administrative structure, processes and communication protocols that must exist in national governments for the implementation of the NETP, and highlights some relevant case studies. Chapter 7 addresses issues related to regulation of communications: specifically, aspects regarding equipment imports, licensing of services, and the administration and planning of radio spectrum. Chapter 8 reviews how different networks and telecom/ICT services can be used in an emergency, and also reviews the literature on technical standards that exist for emergency management. Chapter 9 highlights the importance of continuous training, simulation drills and capacity building for all parties involved in the response to an emergency. Chapter 10 describes the measures and activities that should be considered to help people with specific needs during emergencies, including children, the elderly, and people with disabilities, among others. Finally, in Chapter 11, this document outlines a step-by-step process on how to create an NETP, based on the information presented in the previous chapters.

The document also includes one annex: a checklist to be used during the development of an NETP to ensure that no element is excluded.

## 2. Introduction

According to the United Nations International Strategy for Disaster Risk Reduction - UNISDR, a disaster can be defined as “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”.<sup>2</sup>

---

<sup>1</sup> EM-DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>2</sup> UNISDR Terminology, available at [www.unisdr.org/we/inform/terminology](http://www.unisdr.org/we/inform/terminology) (accessed 20 February 2019).

Consequently, to prevent disaster situations from happening to the extent possible, or to lessen their effects, mitigation and preparedness procedures are required. When a disaster occurs, an immediate response is needed so that the well-being of the affected population can be restored in a timely manner. Telecom/ICTs play a key role in this disaster risk management process: they can support all phases of the disaster, from initial preparedness, early warning (for example, remote monitoring via satellites, radar, telemetry and meteorology, and warning alerts distributed via broadcasting or mobile technology), up to the initial response (radio and television broadcasting, amateur radio, satellite, mobile telephony and the Internet), and the recovery phase (temporary base stations and portable emergency systems) (ITU, 2017c).

Since the end of the eighteenth century, telecom/ICT has been an important part of disaster management, and its use has evolved as new technologies and innovations have become available (Farnham, 2005). Nowadays, the widespread deployment of fixed and mobile terrestrial and satellite communication systems has improved the effectiveness of emergency management and prevention, and has also helped mitigate the negative impacts of disasters and other emergencies.

In line with the evolution of these technologies, recent decades have seen significant advances in global commitment to disaster risk management. For example, the Sendai Framework for Disaster Risk Reduction 2015–2030 (United Nations, 2015a), adopted at the Third United Nations World Conference for Disaster Risk Reduction in March 2015, has raised awareness and aims for increasing resilience of nations and communities to such situations. The 2030 Agenda for Sustainable Development has also helped raise awareness of the importance of disaster and emergency management: of the 17 Sustainable Development Goals established by the United Nations (UN), at least 4 of them (Goals 1, 2, 11 and 13) make reference to the need of nations and communities to improve resilience to disasters (United Nations, 2015b).

In summary, not only have telecom/ICTs become more applicable to disaster risk management over the last several decades, but that evolution has also been accompanied by global agreements to lower risk and improve the response to disasters and other emergencies. To optimize the use of ICTs, it is important for countries to establish an NETPs, to make efficient use of available resources, to minimize the risk of disaster within their borders, to comply with the relevant global agreements and frameworks, and to, as much as possible, avoid economic losses and, above all, loss of life.

### 3. Typology of disasters

It is important to keep in mind that hazards, whether of natural or technological origin, can vary widely in their characteristics. Countries must take into account 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 Caribbean Region is exposed to hurricanes; while a country in Asia with certain hydrographic characteristics could be more exposed








to flooding from rivers, hurricanes and earthquakes; and a European country could face a higher risk of extreme temperatures.

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 chapter addresses variation in the

types of disasters, as classified by the Center for Research on the Epidemiology of Disasters (CRED).<sup>3</sup> CRED categorizes disasters as climatological, geophysical, hydrological, meteorological or technological, among other categories.<sup>4</sup>

**Figure 2: Disaster categories according to CRED**

 Geophysical	 Hydrological	 Meteorological	 Climatological	 Biological
Earthquake	Landslide	Storm	Drought	Animal accident
Mass Movement (dry)	Flood	Extreme temperature	Glacial lake outburst	Epidemic
Volcanic activity	Wave action	Fog	Wildfire	Insect infestation

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

### 3.1. Climatological disasters

Climate-type disasters refer to those caused by long-lived, meso- to macro-scale atmospheric processes ranging from intraseasonal to multidecadal climate variability.<sup>5</sup>

Examples of climatological disasters include droughts and wildfires. A drought can be defined as a “prolonged absence or marked deficiency of precipitation,”<sup>6</sup> or as “a period of abnormally dry

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

<sup>4</sup> 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.

<sup>5</sup> EM-DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>6</sup> World Meteorological Organization – Meteoterm (<https://public.wmo.int/en/resources/meteoterm>).

weather sufficiently prolonged for the lack of precipitation to cause a serious hydrological imbalance”.<sup>7</sup> 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.<sup>8</sup>

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).”<sup>9</sup>



### 3.2. 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.<sup>10</sup>

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.”<sup>11</sup> Earthquakes can occur both on land and below the ocean floor, and in the latter case can generate large ocean waves or tsunamis.<sup>12</sup> 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.”<sup>13</sup>

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.<sup>14</sup>



### 3.3. 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).<sup>15</sup>

---

<sup>7</sup> Ibid.

<sup>8</sup> American Red Cross ([www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies.html](http://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies.html)).

<sup>9</sup> EM-DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>10</sup> Ibid.

<sup>11</sup> World Meteorological Organization – Meteoterm (<https://public.wmo.int/en/resources/meteoterm>).

<sup>12</sup> American Red Cross (<https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies.html>).

<sup>13</sup> World Meteorological Organization – Meteoterm (<https://public.wmo.int/en/resources/meteoterm>).

<sup>14</sup> EM-DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>15</sup> Ibid.

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”.<sup>16</sup>

### 3.4. 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.<sup>17</sup> 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.<sup>18</sup> 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).”<sup>19</sup>

### 3.5. 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.<sup>20</sup>

### 3.6. Historical disasters by region<sup>21</sup>

Table 1 presents a summary of the natural and technological 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.

---

<sup>16</sup> World Meteorological Organization – Meteoterm (<https://public.wmo.int/en/resources/meteoterm>).

<sup>17</sup> EM–DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be/Glossary](http://www.emdat.be/Glossary)).

<sup>18</sup> Ibid.

<sup>19</sup> 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.

<sup>20</sup> The Emergency Events Database – Université Catholique De Louvain (UCL) – CRED (<https://www.emdat.be/classification>).

<sup>21</sup> EM–DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)). All figures belong to the period 1968–2017.

**Table 1: Disasters over the 50 year period 1968–2017**

Type of disaster	Events	Fatalities	Injured	Affected	Homeless	Total affected
<b>Africa</b>						
<b>Climatological</b>	249	505 166	758	361 810 319	32 088	361 843 165
<b>Geophysical</b>	48	2 805	4 224	271 606	253 285	529 115
<b>Hydrological</b>	783	18 178	10 174	56 480 704	3 841 495	60 332 373
<b>Meteorological</b>	212	4 919	14 116	15 944 315	1 852 465	17 810 896
<b>Technological</b>	1 518	56 335	34 624	373 270	216 811	624 705
<i>Total Africa</i>	<b>2 810</b>	<b>587 403</b>	<b>63 896</b>	<b>434 880 214</b>	<b>6 196 144</b>	<b>441 140 254</b>
<b>Americas</b>						
<b>Climatological</b>	292	450	1 637	109 850 315	64 935	109 916 887
<b>Geophysical</b>	299	369 876	675 968	31 476 615	4 274 214	36 426 797
<b>Hydrological</b>	1 221	70 278	55 394	93 387 582	3 801 134	97 244 110
<b>Meteorological</b>	1 240	62 437	1 877 928	152 702 945	3 743 926	158 324 799
<b>Technological</b>	1 301	42 394	57 526	3 213 955	30 237	3 301 718
<i>Total Americas</i>	<b>4 353</b>	<b>545 435</b>	<b>2 668 453</b>	<b>390 631 412</b>	<b>11 914 446</b>	<b>405 214 311</b>
<b>Arab States</b>						
<b>Climatological</b>	65	189 701	15	62 291 213	20 000	62 311 228
<b>Geophysical</b>	37	8 395	33 693	1 399 553	742 234	2 175 480
<b>Hydrological</b>	273	10 965	22 307	12 494 389	2 945 145	15 461 841
<b>Meteorological</b>	73	1 234	6 195	4 188 485	55 960	4 250 640
<b>Technological</b>	714	33 129	25 271	18 988	22 835	67 094
<i>Total Arab States</i>	<b>1 162</b>	<b>243 424</b>	<b>87 481</b>	<b>80 392 628</b>	<b>3 786 174</b>	<b>84 266 283</b>
<b>Asia–Pacific</b>						
<b>Climatological</b>	239	6 536	1 919	2 000 231 872	93 181	2 000 326 972
<b>Geophysical</b>	694	912 236	1 577 007	127 624 985	14 871 692	144 073 684
<b>Hydrological</b>	2 159	253 328	1 245 812	3 463 735 595	79 419 927	3 544 401 334
<b>Meteorological</b>	1 723	773 882	794 663	949 398 926	41 851 503	992 045 092
<b>Technological</b>	3 312	138 405	220 327	1 812 985	680 470	2 713 782
<i>Total Asia–Pacific</i>	<b>8 127</b>	<b>2 084 387</b>	<b>3 839 728</b>	<b>6 542 804 363</b>	<b>136 916 773</b>	<b>6 683 560 864</b>

Commonwealth of Independent States - CIS						
<b>Climatological</b>	38	171	2 319	8 031 194	3 855	8 037 368
<b>Geophysical</b>	42	2 254	2 811	1 027 017	92 086	1 121 914
<b>Hydrological</b>	162	3 731	8 736	5 081 279	306 524	5 396 539
<b>Meteorological</b>	70	58 379	8 876	6 187 536	28 900	6 225 312
<b>Technological</b>	276	8 108	5 218	25 626	10 410	41 254
<i>Total</i>						
<i>Commonwealth of Independent States</i>	<b>588</b>	<b>72 643</b>	<b>27 960</b>	<b>20 352 652</b>	<b>441 775</b>	<b>20 822 387</b>
Europe						
<b>Climatological</b>	126	537	1 213	10 233 832	8 505	10 243 550
<b>Geophysical</b>	168	38 657	118 580	7 626 303	1 688 938	9 433 821
<b>Hydrological</b>	586	6 075	6 145	13 356 770	442 175	13 805 090
<b>Meteorological</b>	665	89 734	23 720	8 684 741	17 603	8 726 064
<b>Technological</b>	855	26 714	51 794	136 976	202 766	391 536
<i>Total Europe</i>	<b>2 400</b>	<b>161 717</b>	<b>201 452</b>	<b>40 038 622</b>	<b>2 359 987</b>	<b>42 600 061</b>
<b>World total</b>	<b>19 440</b>	<b>3 695 009</b>	<b>6 888 970</b>	<b>7 509 099 891</b>	<b>161 615 299</b>	<b>7 677 604 160</b>

## 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 Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

Over the last five decades, 19 440 disaster events were recorded worldwide,<sup>22</sup> 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.<sup>23</sup> 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).

<sup>22</sup> The figures presented throughout the document only consider the five types of disasters described in the section 1.1.

<sup>23</sup> EM-DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

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

#### 3.6.1. Africa<sup>24</sup>

The African continent 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 Africa in terms of frequency, fatalities and total number of people affected.

#### 3.6.2. Americas<sup>25</sup>

From 1968 to 2017, 4 353 disaster events occurred in the Americas 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 American continent 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.

#### 3.6.3. Arab States<sup>26</sup>

More than 1 100 emergency events occurred in the Arab States 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).

---

<sup>24</sup> Based on EM–DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>25</sup> Ibid.

<sup>26</sup> Ibid.

#### 3.6.4. Asia–Pacific<sup>27</sup>

In this 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 losses near 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 in Indonesia, China, Pakistan, the Islamic Republic of Iran, Sri Lanka, etc.).<sup>28</sup> 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.

#### 3.6.5. Commonwealth of Independent States<sup>29</sup>

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.

#### 3.6.6. Europe<sup>30</sup>

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 continent's total death toll.

---

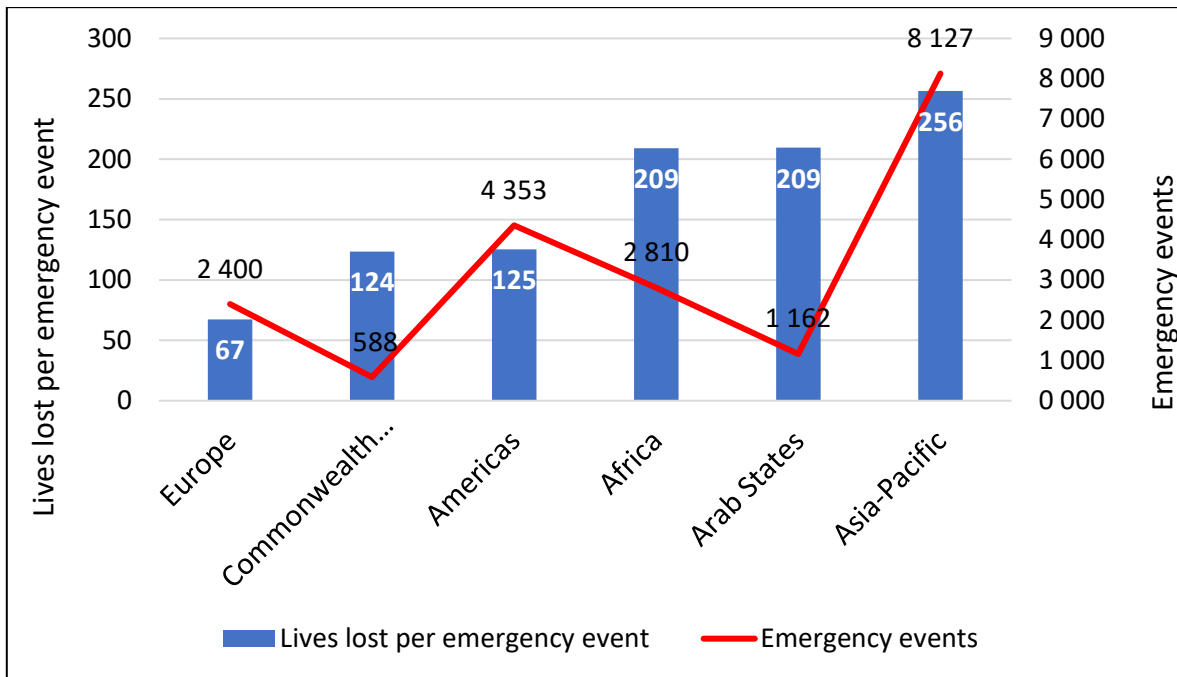
<sup>27</sup> Ibid.

<sup>28</sup> UNISDR, PreventionWeb ([www.preventionweb.net/english/countries/statistics/index\\_region.php?rid=5](http://www.preventionweb.net/english/countries/statistics/index_region.php?rid=5)).

<sup>29</sup> Based on EM–DAT, the Emergency Events Database. Université Catholique De Louvain (UCL) – Center for Research on the Epidemiology of Disasters (CRED), D. Guha-Sapir, Brussels ([www.emdat.be](http://www.emdat.be)).

<sup>30</sup> Ibid.

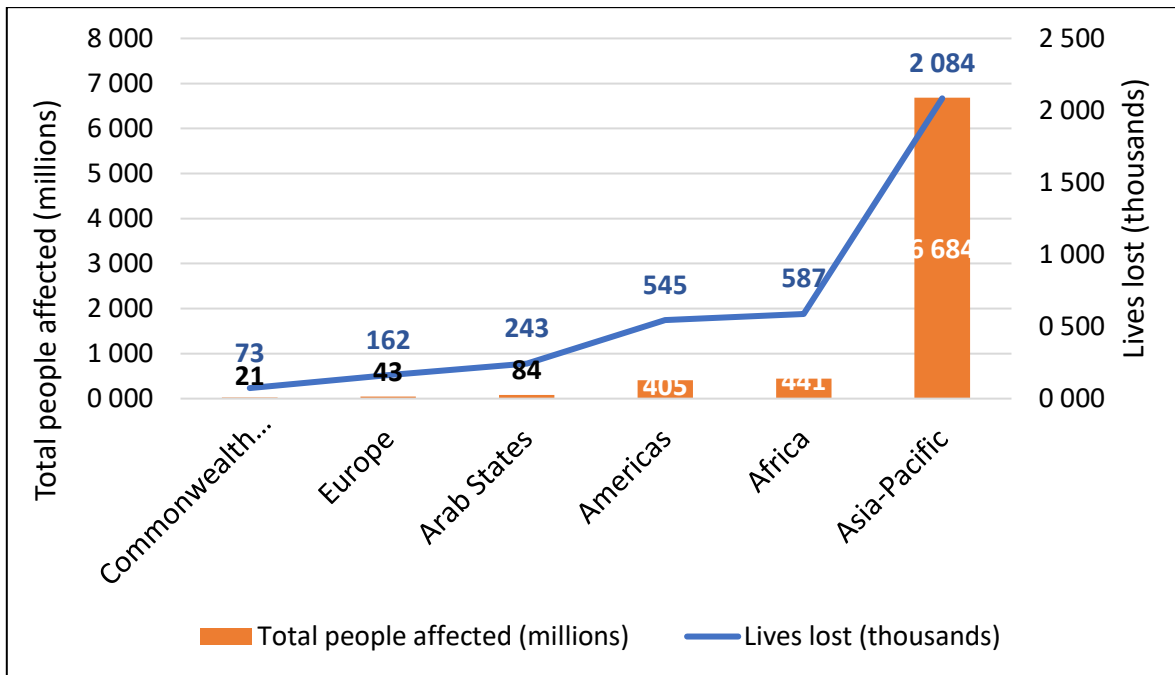
Figure 3: Lives lost per emergency event and number of emergency events in the last 50 years per region



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



Figure 4: Number of people affected (millions) and lives lost (thousands) in the last 50 years per region



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



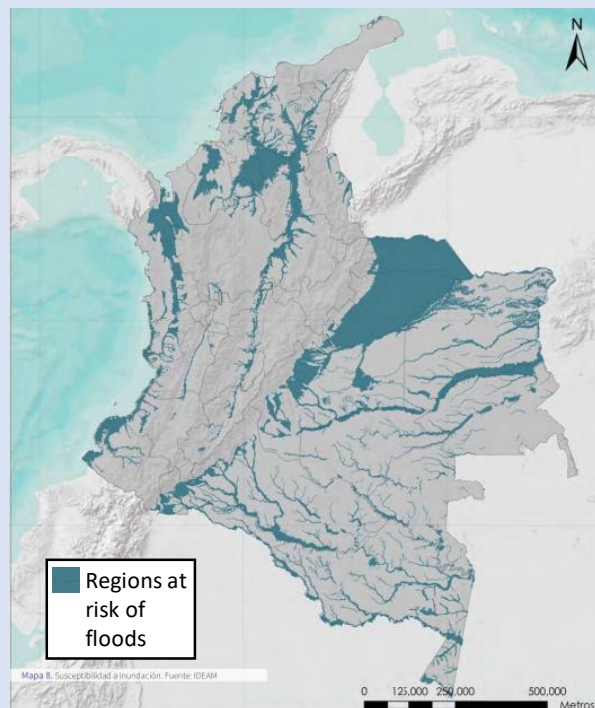
**Recommendation 1:**

Geographic maps depicting the likely locations of possible disasters should be developed and included in the NETP. This is critical for the analysis of telecom/ICT infrastructure risks and contingency plans, as well as for determining the type of warning systems needed.

### Box 1. Case study: Colombia's hazard maps

In Colombia, the National Unit for Disaster Risk Management (UNGRD in Spanish), developed a "Risk Atlas" for the country in November 2018. This Atlas, designed as a tool to improve understanding of the risk of disasters in Colombia, brings together different studies and assessments developed by public and private entities on an array of diverse natural and technological threats, and also makes public the results of the probabilistic risk assessment for different threats based on appropriate risk metrics for decision-making.<sup>31</sup> The Atlas presents, among other elements, maps of floods (as shown in Figure 5), seismic events, tsunamis, tropical cyclones, forest fires and mass movements hazards at the national level. At the departmental level, the Atlas includes multihazard risk profiles with maps of expected annual damages, and the results of the integral risk index, which considers aggravating factors associated with socio-economic fragility, or the lack of resilience at the municipal level.<sup>32</sup>

Figure 5: Hazard map: Floods in Colombia



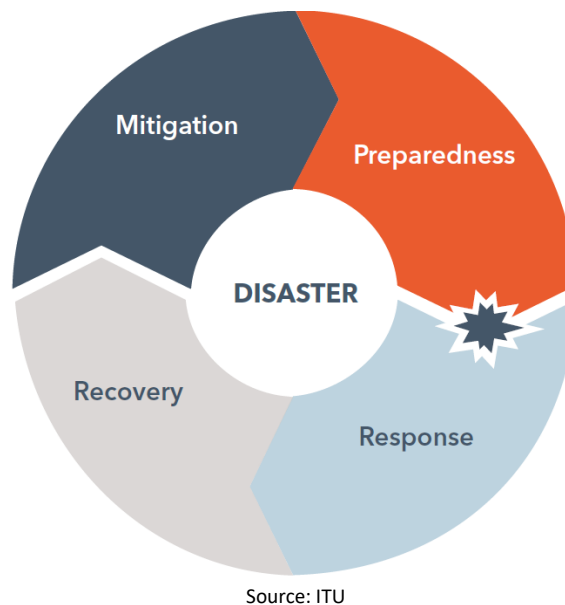
<sup>31</sup> Available at <http://portal.gestiondelriesgo.gov.co/Paginas/Noticias/2018/Colombia-ya-cuenta-con-su-Atlas-de-Riesgo.aspx> (accessed 20 February 2019).

<sup>32</sup> Ibid. The Atlas is available at [www.preventionweb.net/files/62193\\_atlasriesgo1.pdf](http://www.preventionweb.net/files/62193_atlasriesgo1.pdf) (accessed 20 February 2019).

## 4. Phases of disaster management

The disaster management process, adopted internationally by UNISDR, consists of four phases:<sup>33</sup> mitigation, preparedness, response and recovery. As illustrated in Figure 6, the mitigation phase includes aspects such as education and awareness of existing risks, vulnerability assessment and the construction or maintenance of the necessary infrastructure to avoid possible disasters. The preparedness phase considers the establishment of a national emergency telecommunication plan, training, EWSs and operational processes. The response and recovery phases are activated in the event of a disaster, and include aspects of coordination and communication, as well as the restoration of infrastructure and services.

**Figure 6: Disaster management phases**



It is important to emphasize that disaster management has two distinct modes: risk management and crisis management. In the first mode, which corresponds to the mitigation and preparedness phases, measures are taken to predict and give early warning of a disaster, as well as prevent and/or mitigate damage. These efforts occur under ordinary non-emergency conditions.

During and after a disaster, the priority actions become assessment of damage, formulation of a policy response, and the avoidance of a secondary disaster. This second mode corresponds to the response and recovery phases described above.

### 4.1. Disaster mitigation

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

<sup>33</sup> UNISDR Terminology, available at [www.unisdr.org/we/inform/terminology](http://www.unisdr.org/we/inform/terminology) (accessed 20 February 2019).

mitigation phase should be considered and implemented before and after the occurrence of emergency events.

In this phase, telecom/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 support emergency telecom/ICTs, undertaking risk analysis of critical communications infrastructure, taking steps to reduce the vulnerability of telecommunication networks, and improving their resilience (ITU, 2012).

Telecom/ICTs are also used during this phase to coordinate the establishment of infrastructure such as monitoring, early warning and alerting systems; establish procedures to avoid potential threats; and establish mechanisms to raise awareness among citizens. Telecom/ICT and broadcasting play a key role in the dissemination of information on how to mitigate the impacts of and prepare for a potential disaster.

In the same way, these anticipated actions facilitated by telecom/ICT networks and services that seek to avoid risks related to a future disaster can also be used to mitigate climate change or help countries adapt to the effects of climate change. On the one hand, telecom/ICT can be useful to help reduce emissions that contribute to climate change: for example, by replacing travel with videoconferencing, or by helping develop more fuel-efficient forms of transportation. On the other hand, these technologies could also help climate change adaptation by disseminating information to large audiences, for instance, or by helping develop weather forecasting and climate monitoring.

Regarding this last point, computer-based models, such as Remote Sensing or Geographic Information System (GIS) modelling, are now widely used globally to predict long-term climatic changes that can affect the relevant climatic pattern for a given region or country (Akhtaruz and Abdul, 2017). Such long-term predictions can “not only help long-term national plans but also form the basis for long-term development strategies” (ibid.).

In Bangladesh, for example, the Center for Environmental and Geographic Information Service has used Remote Sensing and GIS-based modelling to address areas of research such as weather, environment, climate change impact, and river morphology and erosion, among others. One of these models, in particular, which forecasts medium-term hazards, can predict possible river erosion months before such erosion may take place, preventing the loss of lives and assets in the country. Similar models on rain or drought can also be used to train farmers to grow crops that suit changing weather patterns, or, in other cases, to prevent disaster events produced by these changes in climate well in advance (ibid.).

#### 4.2. Preparedness

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 improvement of coordination and communication between those involved in disaster management. This is achieved through continuous training and mock exercises/drills, as well as activities designed to raise 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 a diverse multistakeholder community when a disaster strikes. Telecom/ICT and other broadcasting services are key to facilitate the dissemination of warnings and alerts so the public is aware of actions they must take during an emergency.

ITU has identified the following points to be included in an NETP in terms of the preparation stage (ITU, 2017c):

- Management and accountability: Establish and clarify the functions, responsibilities and contact points for each government agency and stakeholder.
- External coordination: A disaster communications plan must incorporate all stakeholders, including central government, local communities, state/provincial authorities, public safety officials, the private sector, relief organizations, hospitals, citizen-led groups and civil society organizations, the UN and foreign governments.
- Training and exercises: Training and rehearsal of an emergency response through mock exercises and drills help improve teamwork, prepare teams to respond effectively to a real emergency, enhance knowledge of plans and procedures, and enable members to improve their own performance and identify opportunities to improve system capabilities.
- Infrastructure and technology: One of the objectives of an NETP should be to help ensure the continuity and/or swift re-establishment of communications in a disaster. In particular, during the preparatory phase, an inventory of available technology and energy sources should be carried out. In addition, staff training, spectrum and frequency planning, and other considerations are important, including identifying unmet telecommunication needs and undertaking research on new technologies and methodologies to improve on existing solutions.

### 4.3. Response and recovery

The response phase is the one in which 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, and search and rescue, among other activities. During this phase, a set of activities and procedures is carried out by various entities to connect all actors in the disaster management ecosystem at the local, national and international levels. 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.

The recovery phase, on the other hand, 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. During this

phase, it is especially important that stakeholders work to restore damaged ICT infrastructure as soon as possible, 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.

ITU highlights that, for the phases of response and recovery, the following considerations should be made (ibid.):

- Communication channels and information exchange: When developing a response plan, it is important to understand not only the *channels* of communication available, but also the *types* of information that need to be shared.
- Infrastructure and technology: 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. As such, the report recommends determining in advance, as much as possible, points of contact at relevant stakeholders for 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.

#### 4.4. Principles for the development of an NETP

In order to develop a complete and effective document for all varieties of risk management, an NETP must follow a conceptual guidance and a set of principles, such as the ones shown below:

- Adopt a strategy that addresses all potential hazards to which the nation is exposed.
- Increase awareness and obtain commitment to participation, contribution and agreement on a strategy from all stakeholders.
- Ensure the NETP addresses the linkages between different phases of disaster management and different types of disaster.
- The NETP should include training, drills and evaluation of telecom/ICT infrastructure to be used in all phases of disaster management and at all levels – individual, team, department, and community.
- During NETP implementation, decisions must be based upon accurate assumptions about all potential disaster types.
- SOPs should identify the types of communications/technologies that are required for a given type of emergency.



### 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 telecom/ICT will be helpful in each of these phases. In addition, the development and implementation of the NETP should be governed by a set of principles that include, among others, addressing all of the country's potential hazards, obtaining the contribution from all stakeholders, and the identification of all the communications/technologies that are required for the different emergencies that may arise.

## 5. International cooperation and coordination

International cooperation and coordination are important matters to consider when responding to an emergency. 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.

### 5.1. Emergency Telecommunications Cluster

Clusters are groups of humanitarian organizations, both UN and non-UN, in each of the main sectors of humanitarian assistance: water, sanitation and hygiene; shelter; protection; nutrition; logistics; health; food security; emergency telecommunications; education; early recovery; and camp coordination and management. Each humanitarian organization is designated by the Inter-Agency Standing Committee as part of one or more of these sectors, and has clear responsibilities for coordination with the others.<sup>34</sup> The aim of the cluster approach 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”.<sup>35</sup> It also aims to enhance predictability, accountability and partnerships at the country level by improving prioritization and clearly defining the roles and responsibilities of humanitarian organizations.<sup>36</sup>

The Emergency Telecommunications Cluster (ETC), as part of this cluster system, is currently 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. ETC's main purpose is to provide, within 48 hours of being activated in response to a

<sup>34</sup> Available at <https://emergency.unhcr.org/entry/61190/cluster-approach-iasc> (accessed 21 February 2019).

<sup>35</sup> Available at [www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach](http://www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach) (accessed 21 February 2019).

<sup>36</sup> Ibid.

disaster, vital security communications services, and voice and Internet connectivity, to assist humanitarian workers in life-saving operations.<sup>37</sup>

Among other services, ETC can deploy telecommunication backbones in operational areas, provide voice and data communications around the main centre of operation, provide support via a technical help desk, deploy basic ICT support (connecting to network, printers, etc.), and other coordination and information management activities. In general, what distinguishes ETC from other clusters is that it deploys telecom/ICT during emergencies to provide different services to the people and organizations involved in humanitarian aid, rather than directly to affected populations.<sup>38</sup>

In order to achieve the above, ETC relies on its network of members and partners to carry out its critical work around the world. These members and partners include UN agencies and programmes, NGOs, governments and other humanitarian organizations.<sup>39</sup>

## 5.2. International Telecommunication Union

ITU, created in Paris during the International Telegraph Convention of 1865, is a specialized United Nations agency for telecom/ICT. This body, 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.<sup>40</sup>

During its more than 150 years of existence, ITU has not only helped create a global communications network, which today consists of a wide variety of technologies, but has also made important contributions to the mitigation of disasters, the items to be addressed before potential emergencies and emergency response after a disaster occurs (ITU, 2006b).

The promotion of the global expansion of new technologies such as mobile telephony and the Internet, as well as the management of the radio-frequency spectrum conducted by ITU, has facilitated wireless communication to citizens, both in their daily lives and in times of need during emergencies. The management of radio spectrum, in particular, has allowed an uninterrupted and reliable operation of radio systems, such as mobile phones, radio direction finding devices, air and maritime navigation systems, space research, satellite communications systems, and sound and television broadcasting (*ibid.*), all of which are useful and necessary in disaster management.

Indeed, telecom/ICT plays a key role in environmental monitoring to predict and detect natural disasters, send alerts when a disaster does occur, and ensure the timely flow of information after a disaster has occurred. It does this by ensuring timely flow of information needed by government

---

<sup>37</sup> ETC, available at [www.etcluster.org](http://www.etcluster.org) (accessed 21 February 2019).

<sup>38</sup> *Ibid.*

<sup>39</sup> ETC members and Observers, available at [www.etcluster.org/etc-members-and-observers](http://www.etcluster.org/etc-members-and-observers) (accessed 21 February 2019).

<sup>40</sup> About International Telecommunication Union (ITU), available at [www.itu.int/es/about/Pages/default.aspx](http://www.itu.int/es/about/Pages/default.aspx) (accessed 21 February 2019).



agencies, humanitarian-oriented organizations and industry involved in rescue, recovery and providing medical assistance (ITU, 2013).

Besides promoting the development of telecom/ICT and spectrum 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). Beyond the original commitment in its Constitution, ITU has also shown the priority it places on the effective use of telecommunications during disaster and emergency response 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 (ibid.).

In order to fulfil these mandates, ITU, among other activities, 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 contributes to the specifications in the Emergency Telecommunications Service, the International Emergency Preferences Scheme and a Common Alerting Protocol (CAP) (ITU, 2013).

Finally, ITU also cooperates closely with the United Nations Emergency Relief Coordinator and the chief of the Office for the Coordination of Humanitarian Affairs (OCHA), and acts as a member of the Working Group on Emergency Telecommunications, fulfilling the role of “consultative board” within the framework of the Tampere Convention (ITU, 2006b).

### 5.3. Tampere Convention

The Tampere Convention<sup>41</sup> is designed to facilitate the use of telecommunication resources for disaster mitigation and relief. The treaty establishes a framework for international cooperation for states, non-governmental entities and intergovernmental organizations.<sup>42</sup> 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

---

<sup>41</sup> The Convention emerged out of an assembly of 225 delegates from 75 countries in the city of Tampere, Finland, in 1998. It subsequently entered into force on 8 January 2005, just two weeks after the devastating Indian Ocean tsunami. It has currently been ratified by 36 countries. See Tampere Convention, available at [www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere\\_Convention/Tampere\\_convention.pdf](http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf) (accessed 21 February 2019).

<sup>42</sup> “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).

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; and
  - 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.

In summary, the Tampere Convention provides a legal framework for using telecommunications within the scope of international humanitarian assistance. This framework 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 telecom/ICT 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.<sup>43</sup>

The above is important considering that, in many countries, legislation continues to hinder (or even prohibit) the arrival and timely installation of communications equipment in affected territories. Restrictive laws applied to imports, for example, can leave humanitarian agencies without access to basic communications equipment during search and rescue operations.<sup>44</sup> Similarly, organizational barriers can impede the flow of information between the various elements of the international disaster response network, or in some cases, high costs may inhibit the effective use of communications equipment during emergencies.

A country can express its consent to be bound by Tampere Convention by any of the following means:<sup>45</sup>

- By signature (definitive signature);
- By signature subject to ratification, acceptance or approval, followed by the deposit of an instrument of ratification, acceptance or approval;
- By deposit of an instrument of accession.

Ascension to the Convention, open to any member State of the United Nations or ITU, comes into force 30 days after the deposit of instruments of ratification, acceptance, approval, accession or definitive signature of thirty (30) States.<sup>46</sup>

In order to avoid the previous limitations and disadvantages, as well as to maximize benefits from the agreement, a country can express its consent to be bound by the Tampere 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 particular articles of the treaty. 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.

<sup>43</sup> Tampere Convention, available at [www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere\\_Convention/Tampere\\_convention.pdf](http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf) (accessed 21 February 2019).

<sup>44</sup> Ibid.

<sup>45</sup> United Nations Treaty Collection, available at [https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=XXV-4&chapter=25&clang=\\_en](https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXV-4&chapter=25&clang=_en) (accessed 21 February 2019).

<sup>46</sup> Ibid.

It is also 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's terms and procedures and have a clear knowledge of the framework.

Finally, the Convention has binding force for those 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 (*ibid.*).

#### 5.4. 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.<sup>47</sup>

OCHA is not an operational agency directly involved in the delivery of humanitarian programmes. Instead, it acts as an “honest broker, facilitator, thought leader and global advocate, providing support to the humanitarian system”. OCHA also designs frameworks to coordinate the contribution of all actors to the overall response effort.<sup>48</sup>

OCHA also acts as the Tampere Convention's global operational coordinator<sup>49</sup> and, as such, it has a number of tasks aimed at improving coordination and information sharing with regard to telecommunication assistance (International Federation of Red Cross and Red Crescent Societies, 2011). 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.<sup>50</sup>

---

<sup>47</sup> United Nations Office for the Coordination of Humanitarian Affairs, available at [www.unocha.org/about-us/who-we-are](http://www.unocha.org/about-us/who-we-are) (accessed 21 February 2019).

<sup>48</sup> *Ibid.*

<sup>49</sup> Tampere Convention, available at [www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere\\_Convention/Tampere\\_convention.pdf](http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf) (accessed 21 February 2019).

<sup>50</sup> *Ibid.*

### 5.5. United Nations International Strategy for Disaster Reduction

The United Nations General Assembly appointed UNISDR as the secretariat of the International Strategy for Disaster Reduction in December 1999, and determined that UNISDR would guarantee the implementation of this strategy. In 2001, the mandate of UNISDR was extended to include serving 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.<sup>51</sup>

UNISDR, as the UN office for disaster risk reduction, supports the implementation, follow-up and review of the Sendai Framework for Disaster Risk Reduction 2015–2030. This framework was adopted by the Third United Nations World Conference on Disaster Risk Reduction on 18 March 2015 in Sendai, Japan. It is a voluntary, non-binding agreement that traces an approach to disaster risk reduction, succeeding the Hyogo framework of action, which was in effect from 2005 to 2015.<sup>52</sup>

The Sendai framework provides guidelines for natural disaster prevention, preparedness and mitigation, among other things. Additionally, the Sendai Framework contains new innovations not contained in the previous framework, including, “[emphasis on] disaster risk management as opposed to disaster management, the definition of seven global targets, the reduction of disaster risk as an expected outcome, a goal focused on preventing new risk, reducing existing risk and strengthening resilience, as well as a set of guiding principles, including primary responsibility of States to prevent and reduce disaster risk, all-of-society and all-of-State institutions engagement” (United Nations, 2015a).

Likewise, the Sendai Framework extended the scope of the previous framework to include both natural and manmade hazards and the associated environmental, technological and biological hazards and risks (ibid.).

The UNISDR vision is based on four priorities established under Sendai:<sup>53</sup>

- Evaluate the risk of disasters;
- Strengthen management of disaster risk;
- Invest in disaster risk reduction in order to build resilience; and
- Improve preparation before disasters in order to achieve positive outcomes.

Additionally, UNISDR’s 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” (United Nations, 2015a).

---

<sup>51</sup> UNISDR, available at [www.unisdr.org/who-we-are/mandate](http://www.unisdr.org/who-we-are/mandate) (accessed 21 February 2019).

<sup>52</sup> Ibid.

<sup>53</sup> UNISDR, Chart of the Sendai Framework for Disaster Risk Reduction 2015-2030, available at <https://www.unisdr.org/we/inform/publications/44983> (accessed 21 February 2019).

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

### 5.6. Bilateral agreements

Many of the existing international instruments for disaster response are in the form of bilateral treaties and agreements. 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 telecom/ICT in particular, 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 (ITU, 2006a). Also, bilateral or multilateral agreements can be useful for countries where specific telecom/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 telecom/ICT, capacity building or training on the use of equipment during the mitigation and preparedness phases, and deploying relief personnel or telecom/ICT experts during the response and recovery phases.



#### **Recommendation 3:**

The NETP should include a description 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 adhere to the Tampere Convention and to take the necessary actions at national and local level to ensure that the Convention will be effective in a disaster situation.

## 6. National disaster management

Clear administrative structures, processes and communication protocols are essential to the satisfactory implementation of an NETP. The establishment of clear policy and implementation frameworks is important not only for government agencies, but also for the organization and coordination of all 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.

### 6.1. 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 coordination mechanisms, communication channels and SOPs, 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 (ibid.).

To develop an NETP, a country should start with the assumption that there is national legislation 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 nature essential.<sup>54</sup> Likewise, planning must start 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.

In addition to the above, the development and implementation of an NETP necessitate a specific set of policies on emergency communications that support or supplement national legislation in the implementation of a comprehensive national approach. These policies must be designed to establish, develop or improve national interoperable telecommunication capabilities. Regulatory authorities and the government must have the mandate to issue the proper rules and regulations, both technical and legal, corresponding to the implementation of national laws. National stakeholders, including telecom 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 and regulations.

While the national legislative framework and specific policies and regulations form the basis for an NETP, the plan must also define the methodologies and chain of command that will guide all stakeholders in the event of an emergency. An emergency telecommunication plan, specifically, is a cross-cutting plan, supporting response at all levels during an emergency, and should describe how 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 (national legislation, specific policies, regulations and plans), the next step for a country should be to develop SOPs: that is, more detailed instructions on how to carry out the specific operational tasks or activities of emergency response. These strategies, plans and operating procedures must be designed to promote a standardized and uniform response during emergency response operations, and standardize use and application of

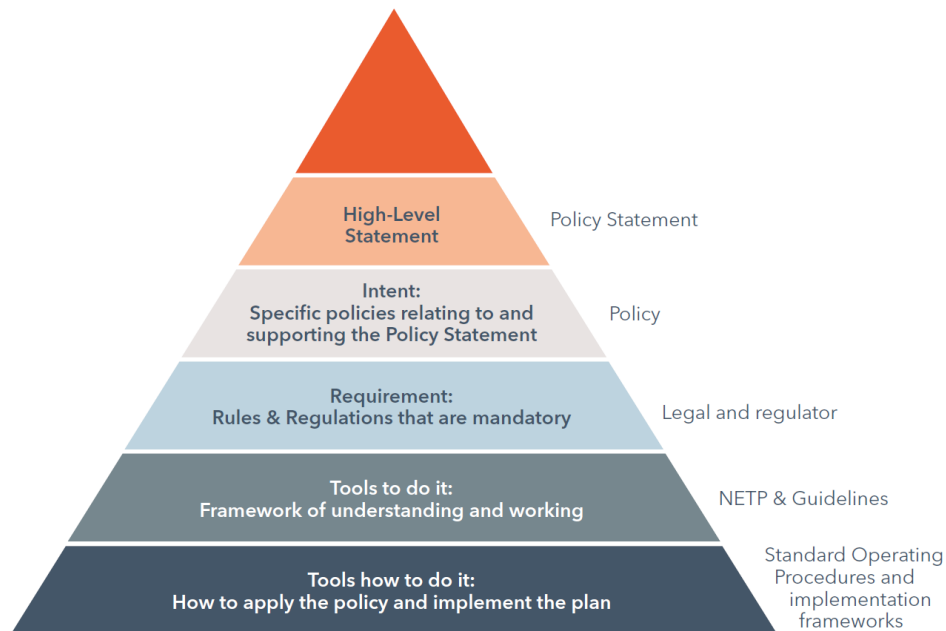
---

<sup>54</sup> UNISDR, available at [www.unisdr.org](http://www.unisdr.org) (accessed 21 February 2019).

interoperable emergency communications terminology, backup solutions and systems (United States Department of Homeland Security, 2014).

These SOPs, in addition, are critical, as they can help all levels of government manage their future emergency communication asset requirements and capabilities, as well as the deployment of new mobile data services and applications. In that context, responding agencies should assess their needs for strategic, commercial, operational and tactical planning on a regular basis, and update them periodically (ibid.).

**Figure 7: Steps of NETP development and implementation**





**Box 2. Case study: Safecom’s Writing Guide for Standard Operating Procedures<sup>55</sup>**

The United States Department of Homeland Security agency Safecom<sup>56</sup> 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, Safecom’s guide offers general direction on how SOPs should be developed, and includes clear recommendations on how they should be structured.

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.

## 6.2. Administrative structure and governance model

There are a large number of diverse stakeholders involved in the different phases of disaster management. If there is to be an effective preparation and response, there should be a well-defined structure involving all stakeholders. This includes both national and international stakeholders, within the territory where the emergency is likely to occur or has occurred. Likewise, there must be a clear model of government that allows planning, executing and revising the activities to be carried out.

The disaster management process must take place under the leadership of the national government, which defines the responsibilities and procedures for all 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 regional, departmental, municipal and local levels. In the elaboration of emergency and disaster care plans, distinctions can be made between the following: (a) national plans, (b) sectoral plans and (c) institutional plans.

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

---

<sup>55</sup> Based on United States Department of Homeland Security (N.D.).

<sup>56</sup> Available at [www.dhs.gov/safecom/about-safecom](http://www.dhs.gov/safecom/about-safecom) (accessed 21 February 2019).

**Box 3. Case Study: Colombia’s administrative structure and governance model<sup>57</sup>**

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.

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 telecom service providers within each level of the response hierarchy.<sup>58</sup>

This need for coordination between all national actors also applies to international humanitarian assistance. The government of the country where the disaster occurred is the main interface with foreign aid agencies, whose activities must be fully integrated with decision-makers at local and regional levels. Also, emergency clusters<sup>59</sup> can play a key role in the coordination of a response to a disaster by uniting agencies to work together towards common objectives within a particular sector of emergency response.<sup>60</sup> In particular, telecommunication clusters can provide services during a crisis and improve communications resilience and local capacity. For example, ETC, led by WFP, is a global network of humanitarian, governmental and private sector organizations that work together

<sup>57</sup> Available at <http://portal.gestiondelriesgo.gov.co/Paginas/Estructura.aspx> (accessed 21 February 2019).

<sup>58</sup> Ibid.

<sup>59</sup> 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](http://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/](http://www.who.int/hac/techguidance/tools/manuals/who_field_handbook/annex_7/en/) (both accessed 21 February 2019).

<sup>60</sup> World Health Organization, available at [www.who.int/hac/techguidance/tools/manuals/who\\_field\\_handbook/annex\\_7/en/](http://www.who.int/hac/techguidance/tools/manuals/who_field_handbook/annex_7/en/) (accessed 21 February 2019).

to provide timely, reliable and effective telecommunication services to humanitarians responding to crises.<sup>61</sup>

Putting in place a structure of disaster response prior to a disaster is key to saving lives and reducing impacts, as well as alleviating the suffering of those who survived the disaster, because at the moment a disaster strikes, devastating effects can be widespread in a matter of seconds, minutes or hours. Also, it is vital to consider that organizing agency contacts and designating key contact points and leaders of a response have also been applied in some countries and regions to address alert and early warning systems and procedures in the phases prior to a disaster. Additionally, this kind of coordination during the mitigation and preparation phases can be especially important in facilitating drills and exercises.

Consequently, the free flow of information, collaboration and cooperation between entities within the national emergency response team is vital during any disaster management phase. In order to facilitate the effective response to incidents, threats or disasters, national communications infrastructure should always be available, provide interoperability at any time, and should offer flexibility to those who rely on it before, during and after disasters. It is important to consider that, when a disaster occurs, the national communications infrastructure may be damaged or even completely destroyed, further underscoring the importance of developing redundant and separate disaster management communications infrastructure.

Along with the organizational structure, both vertical and horizontal, that describes how cooperation between the parties should function, disaster risk management also requires the establishment of a clear governance model to support all phases of disaster management. This model must be aligned with national emergency management frameworks, plans and policies. Strong government leadership in the form of comprehensive and inclusive formal inter-institutional structures, established protocols for communication and decision-making, and strategic planning processes are all essential to this process.

---

<sup>61</sup> See also section 5.1. Source: World Food Programme, Emergency Telecommunications Cluster, available at [www1.wfp.org/emergency-telecommunications-cluster](http://www1.wfp.org/emergency-telecommunications-cluster) (accessed 21 February 2019).

**Box 4. Case Study: The United Kingdom’s administrative structure and organizational model<sup>62</sup>**

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 telecom infrastructure of the United Kingdom. The document designates the Department for Business, Innovations and Skills as the lead Government Department for telecom policy, as well as establishing points of contact within the Department and outlining the role for industry.

In particular, according to the Plan, the Department for Business, Innovations and Skills is responsible for leading the response to an emergency involving telecoms, and shall serve as the key link for information flow between the telecom 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’s 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 Telecoms 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 telecom 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 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 Plan offers some guidelines regarding spectrum management issues so that, depending on the severity of the emergency, Ofcom, the United Kingdom’s communications regulator, could increase flexibility in licensing matters and the use of frequencies.

Among other activities, proper governance includes keeping information up to date on the staff and resources available, as well as sharing that information (in advance) with all stakeholders, such as

---

<sup>62</sup> United Kingdom, 2010.

fire and police departments, among others. Likewise, the government must make a needs assessment to define specific areas of focus for capacity building and exercises, including resource assignments and drills. Likewise, after exercises or drills, facilitators must also conduct a debriefing and prepare reports on lessons learned, challenges faced, suggested solutions and corrective action plans, and integrate these into the plans and procedures that make up the telecommunication emergency programme.

The governance aspect of an NETP should also include permanent telecommunication funding allocated for major disasters based on the risk profile of the country. These funds should only be accessible for use during emergency situations to better assist initial recovery efforts. Funds should also be specifically earmarked for emergency telecommunications due to the crucial role they play in emergency response and coordination.

Finally, effective governance also necessitates accountability, transparency and meaningful participation in all procedures and practices. A lack of accountability implies greater leeway for corruption, increasing existing risk factors (UNISDR, 2018).

### 6.3. Public–private cooperation, coordination, communication and contingency plans

Preparation for emergencies is more effective when plans are made jointly by public authorities and the private sector.

However, due to the liberalization and privatization of telecommunication networks, many private sector companies may worry that sharing information about the capacity of a network may give a commercial edge to a competitor and exhibit reluctance when it comes to sharing information related to network capacity. Additionally, many companies have a continuity plan, which explains in detail the location of spare parts and the logistics for the rapid restoration of services and the revalidation of data. This information may be of interest to potential saboteurs. As a result, telecommunication organizations may not wish to provide information, even if they agree with the ultimate goal of disaster preparedness (ITU, 2001).

Consequently, it is important that State authorities leading emergency response keep lines of communications with the private sector open, develop trust and build capacity for cooperation. It is possible, for example, that network operators are willing to deliver sensitive information only to a select group of people (usually at the highest levels of the agencies and entities involved). 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 can also establish a set of laws or

regulations in order to ensure that the required cooperation from private stakeholders is available when needed.

**Box 5. Case study: Chile’s regulations on telecom networks for emergency management<sup>63</sup>**

The Government in 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<sup>64</sup> 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 forced to maintain redundancy 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 telecom/ICT network infrastructure for emergency telecommunications and make periodic reports to the Secretary of Communications.

To develop and implement an effective NETP, it is necessary that all national agencies and stakeholders dealing with emergencies participate in and contribute to ensuring the availability of telecom/ICT for disaster management. This way, all stakeholders involved in emergency coordination can be aware of the challenges they might face, and measures taken to address them.

#### 6.4. Communication channels

In order for coordination mechanisms to work across the various parties involved in disaster management at the national level, reliable and continuous communications are required. Although some of the objectives of an NETP focus on developing capacities to achieve operational and interoperable communications, it is also essential to translate those elements into operational success; that is, ensuring that communications planning, processes, partnerships and resources are

<sup>63</sup> Ministry of Transport and Telecommunications of Chile, Decree 125 of 2013.

<sup>64</sup> 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”.

effectively coordinated and utilized during response and recovery operations (United States Department of Homeland Security, 2014). Although responders require communications to achieve their mission under all circumstances, the need for interoperable and continuous communications capabilities for all stakeholders is especially urgent during large-scale disasters and catastrophic situations (ibid.).

To achieve this continuity of communication services, it is important to use all available means of communication, maintain close coordination with the various agencies involved, and design regulatory frameworks with clearly delineated responsibilities. This coordination with, for example, international agencies, can help responders obtain communications equipment that is not available locally.

### 6.5. Contingency plans

Contingency planning is an important part of disaster risk management and should be considered when developing an NETP. In particular, a contingency plan regarding telecommunications for disaster management implies establishing operational procedures (resources and capacity) in order to respond to possible disasters in a specific area. This possible scenario is associated with the specific or known risks in that particular location: for example, a flood, earthquake or any other hazard identified for that area. With this in mind, a contingency plan should include specific procedures, depending on the unique characteristics of that location, such as the level of connectivity of the site, or the available telecom/ICT facilities or equipment 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 preparedness for a timely and effective response, a contingency plan is intended to anticipate an event based on *specific 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) 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 must 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).

### 6.6. Definition of roles and identification of contact points

Another essential issue to consider is that each of the institutions involved in disaster response must 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 and Social Protection 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 SOPs for the different types of emergencies that 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 those with the power to make decisions 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 4:**

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 the national disaster risk management plan.

## 7. Telecom/ICT legislation and regulation

Telecom/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 telecom/ICT policies for disaster management needs to be in place. Regulatory authorities and government have the mandate to issue adequate rules and regulations to implement the national law or set of laws. Such rules and regulations must describe in detail the responsibilities, protocols and strategies each stakeholder – including telecom/ICT operators, public and private organizations, government and the community – must implement to effectively and efficiently use, provide or facilitate emergency telecom/ICT services during national disasters.

## 7.1. 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 must 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 ultimately saving lives and reducing the negative impact of a disaster.
- Establish a new government entity or charge an existing one 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 President, telecom/ICT ministry or regulator. This entity must also be responsible for the overall coordination 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, regulatory agencies and first responders, among others: The entity must also have authority to collaborate with the private sector, including telecom/ICT operators, private networks, amateur radio, etc.
- Define the government 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 must empower government entities with legal tools to prepare for a disaster and also manage requests from government institutions and the private sector, e.g. to develop (a) telecom/ICT national network infrastructure maps; (b) disaster risk and vulnerability maps; (c) specific telecom/ICT regulation such as temporary licensing, type approval, import/export of telecom/ICT equipment, and priority call routing; and (d) international cooperation agreements.

## 7.2. Regulation

Telecom/ICT regulation for disaster management must be in place before a disaster occurs and should be aimed at reducing 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 telecom/ICT services to be available as soon as possible, e.g. waive or expedite temporary licenses and type approvals, reduce any barriers for import/export of equipment, grant temporary spectrum permits and suspend spectrum/license fees, among other actions. The NETP should promote and include all ITC/telecom regulations in the following subsections:

- Telecom/ICT services licensing:

During a disaster, the telecom/ICT regulatory authority must have the power to quickly grant telecom/ICT service licenses it deems necessary to support emergency telecom/ICT efforts. Therefore, exceptional expedited licensing procedures should be in place, free of charge, for use in emergency situations. These licenses should be temporary and valid only during the period of disaster response and recovery, until such time as the government has determined that there is no further need for the 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 radiocommunication networks.

Broadband radiocommunication 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 should 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.

A combination of spectrum bands should be available free of charge for emergency communications, allowing both terrestrial and satellite systems<sup>65</sup> to be quickly deployed with limited interference, in case a disaster occurs. For example, the C-band is critical for satellite systems worldwide for emergency communications. In addition, spectrum for mobile terrestrial services is also critical in the lower bands – for example, 400, 700, 800 and 900 MHz bands – using different technologies such as TETRA, P25 and LTE.

- Priority call routing:

During emergencies, networks fail to provide service for different reasons: e.g. power outages, infrastructure collapses and overloaded networks, among others. As a result, networks become congested, delaying or altogether preventing critical communications between first responders. Regulations must 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 telecom/ICT outages in the event of an emergency. Disaster networks need to consider redundancy and resilience in their design, as well as increase the number of terminals. Regulators need to ensure

---

<sup>65</sup> - Radiocommunication RS.1859 (2010), *Use of remote sensing systems for data collection to be used in the event of natural disasters and similar emergencies*.ITU (2010). This recommendation provides the frequency bands used in remote sensing for disaster prediction and detection.

that telecom/ICT providers have networks with the adequate redundancy and multiple connectivity options.

- Type approval of telecom/ICT equipment:

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

- Importing telecom/ICT equipment:

Major delays during the importation of telecom/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 duties or tariffs, restrictions based on local standards, extensive paperwork, disorganized processes, etc.

Rules should be in place to expedite the importation process of critical telecom/ICT equipment for disaster response and recovery: e.g. exemptions from duties and tariffs, clear expedited processes and streamlined paperwork.<sup>66</sup> 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. Case study: Peru's regulations for telecommunication services during emergency situations<sup>67</sup>**

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 system includes (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. Below is a description of the government provisions:

<sup>66</sup> For more detail, see the Tampere Convention in section 5.3.

<sup>67</sup> Ministry of Transportation and Communications of Peru (2007).

(a) Special communications network for emergency situations:

Fixed and mobile telephony providers must reserve network capacity permanently and free of charge to be used by the authorities. Once an emergency is present, this network will be immediately activated and available to the authorities.

(b) Guidelines for disaster prevention:

Fixed and mobile telephony providers must implement and enable the emergency number (119) for voice messaging and promote short message service (SMS) as an alternative to telephony communications during emergency situations. Emergency agencies – such as, police, civil defence, firefighters, etc. – must adequately size their network capacity, e.g. lines and access trunks, in order to offer an efficient service when call demand is high, as in during emergency situations. Telecommunication providers and amateur radio operators must perform periodic emergency drills together.

(c) Guidelines for action during emergency situations:

During emergency situations, a fixed range of between 1 and 2 minutes for mobile and fixed phone calls for the public is required. However, this requirement does not apply to calls within the special communications network for emergency situations to be used by the authorities. In addition, calls to emergency numbers must be free during the disaster.

Local and long-distance backbone providers must have redundancy networks in order to handle traffic from other providers that experience difficulties after an emergency.

Broadcasters are required to support communication and messaging strategies to the affected population during emergency situations, in coordination with MTC.

Amateur radio operators will provide telecommunication support in the affected areas in coordination with the Government.

(d) Guidelines for response in affected areas:

In affected areas and during an emergency, fixed and mobile telephony providers must offer voice calls free of charge. Telecommunication providers must also deploy wireless network infrastructure, e.g. portable base stations and terminals, which will be made available to MTC free of charge.

MTC must adopt a more flexible approach to issuance of authorizations for the use of the radio spectrum, and of the technical characteristics necessary for the operation of telecommunication services in the affected areas. Under certain circumstances established by MTC, the infringements and sanctions regulatory framework will not apply during emergency situations.

(e) Promotion of amateur radio operators:

Type approval is not required for equipment to be used by amateur radio operators. In addition, the authorization, renovation and change of category fee for radio amateur operators will be equivalent to 0.1 per cent of a tax unit. The authorization is valid for one year.<sup>68</sup>



#### Recommendation 5:

Legislation and regulation regarding telecom/ICT for disaster management should be in place and described in the NETP. Such legislation must provide general high-level guidance on the development of the NETP, while still allowing flexibility during its construction and implementation.

Telecom/ICT regulation regarding temporary licensing, type approval, import/export of equipment, frequency allocations, network redundancy and priority call routing, among others, should be enacted and enforced.

A description of both the legislation and regulation on telecom/ICT for disaster management must be included in the NETP.

## 8. Telecom/ICTs for emergencies<sup>69</sup>

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

However, telecom/ICT services are only effective to the degree that people who need to act receive the information that allows them to protect lives and livelihoods. In recent decades, a standardized emergency messaging format, the Common Alerting Protocol (CAP), has been increasingly adopted. This simple but general format<sup>70</sup> 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 4 in its provision that the NETP includes communication protocols essential to implementation.

Ideally, leveraging the CAP standard at any level (community, city, county, providence, country, region) should be well coordinated among all the major actors in emergency management. This

<sup>68</sup> One tax unit was equivalent to approximately USD 1 245 as of October 2018.

<sup>69</sup> These sections are mainly based on ITU (2007a), *Compendium of ITU's work on Emergency Telecommunications*. It is recommended to refer to said document for additional information on any of the topics presented.

<sup>70</sup> ITU (2007b), Standard X.1303 (<https://www.itu.int/rec/T-REC-X.1303>). Additional information and references about the Common Alerting Protocol (CAP) standard are available at [www.preparecenter.org/resources/cap](http://www.preparecenter.org/resources/cap) (accessed 21 February 2019).

includes the commercial sector as well as governmental and non-governmental sectors. These various actors have many complementary and sometimes overlapping roles, ranging from alert origination through dissemination to adaptive emergency response using dynamic feedback.

This chapter describes the different public and private telecom/ICT services – including radio and television (TV) broadcasting services, among others – that should be considered in the development of an NETP. It also discusses 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 telecom/ICT networks; a vulnerability and risk analysis of all telecom/ICT networks; and network contingency plans for when emergencies and disasters occur. Finally, this chapter addresses the elements that must be considered in EWSs. It includes a description of the standardized emergency format CAP.

## 8.1. Telecom/ICT services

The term “public services” refers to services offered through telecom/ICT networks to which ordinary citizens have access, while the term “private services” refers to services offered through telecom/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.

### 8.1.1. Public telecom/ICT services

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

#### *Public telecom/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.

Both the local loop or the WLL have advantages and disadvantages in the event of a natural 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. When power supply is interrupted, the communication service is also interrupted, because the radiocommunications equipment in the home will not be able to work.<sup>71</sup> 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 natural 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 telecom/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 events, such as floods, earthquakes, etc. In this case, the telecom/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.

---

<sup>71</sup> Unless there is an alternative power supply, e.g. UPS, which is not common.



2. Allow high-priority users to avoid the queue and obtain the next available circuit.
3. Eliminate some users to continue to serve high-priority users.

The implementation of any of these options must be coordinated with regulatory entities. In fact, in many cases, the regulatory authority defines the strategy to be implemented.

- 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 disasters 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 maintain adequate redundancy systems.

#### *Public telecom/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, telecom/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.<sup>72</sup> 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 natural disasters. This is

---

<sup>72</sup> 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.

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, like 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.

RBSs for mobile networks are connected to mobile exchanges through microwave links, optical fibre, or wired networks, similar to fixed networks. Likewise, mobile exchanges are also vulnerable to power failure. Typically, when power supply is interrupted, RBSs remain operational for eight additional hours, using on-site batteries.

There are also so-called “cells on wheels” or COW RBSs. These are mobile base stations that can be rapidly installed in specific locations to increase coverage and capacity when required.

During an emergency or disaster, mobile networks, like 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 natural 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 safety organizations can plan response strategies, and provide updated and accurate information to the public.<sup>73</sup>

---

<sup>73</sup> United States Department of Homeland Security (2013). This document contains several social media implementation methods.

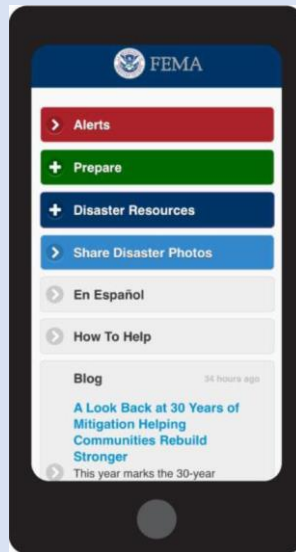
### Box 7. Case study: United States Federal Emergency Management Agency Mobile App<sup>74</sup>

The Federal Emergency Management Agency (FEMA) Mobile App contains:

- Real-time alerts from the National Weather Service;
- Emergency safety tips for over 20 types of disasters;
- Interactive emergency kit list, emergency family plan and reminders;
- Emergency meeting locations;
- Map with open shelters and disaster recovery centres.

The app also has a “disaster reporter” feature allowing people to take and submit Global Positioning System (GPS) photo reports of disasters, so they can be displayed on a public map for others to view.

Figure 8: FEMA’s Mobile App



#### *Public telecom/ICT services via satellites*

Terrestrial communications services through mobile or fixed networks can be seriously affected after a natural disaster. The communication towers, telephone exchanges, utility posts and power

<sup>74</sup> United States Federal Emergency Management Agency, available at [www.fema.gov/mobile-app](http://www.fema.gov/mobile-app) (accessed 22 February 2019).

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.

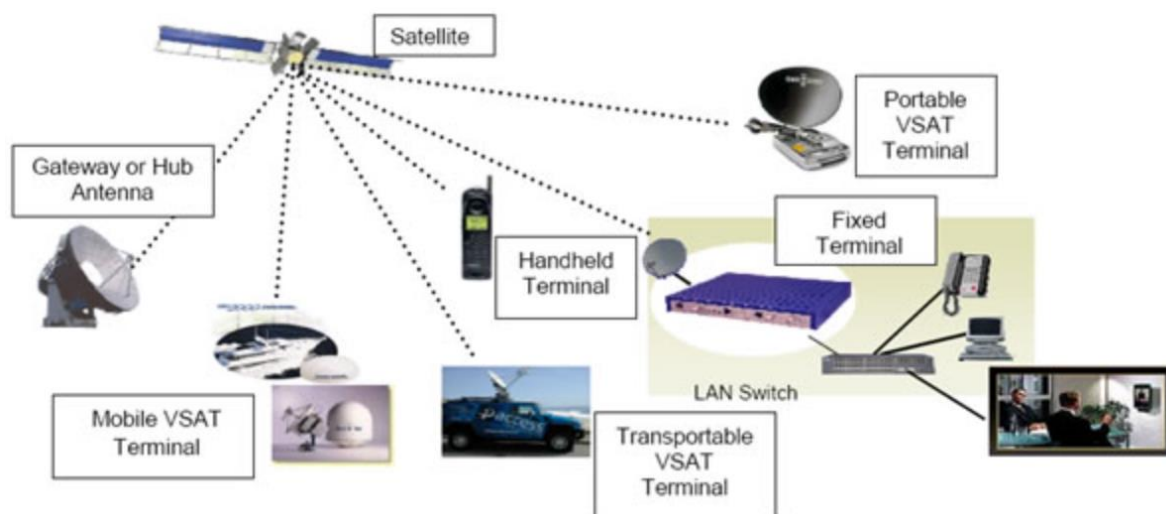
Nowadays, satellite networks provide various communications services: voice, data and video, through broadband connectivity, for example. These services can be classified into mobile satellite service (MSS) and fixed satellite service (FSS). Additionally, satellite services are classified into two types 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.

Today, satellite data services offer narrowband and broadband solutions, with access speeds from 64 kbit/s to 40 Mbit/s, offered on hardware from handheld devices to portable VSAT (Very Small Aperture Terminal) systems, as well as satellite access facilities.

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 9: Satellite systems**



### 8.1.2. Private telecom/ICT services

Private telecom/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 offer six different modes of operation: direct mode between terminals; network mode, in which there is a network with base radio stations and switching centres; dual surveillance, in which the terminal operates in both direct mode and network mode; repeater mode, in which it is possible to expand the coverage area; gateway mode, which allows interconnecting two incompatible systems; and ad hoc mode, in which there is no infrastructure used and it is the terminals that fulfil the function of routing the information.

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; (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 natural disaster has affected the available transit pathways.

### 8.1.3. 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.<sup>75</sup> Social media such as Facebook, Instagram, WhatsApp, among others, will reach nearly 2.8 billion users worldwide in 2019.<sup>76</sup> 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 telecom/ICT networks. In other words, it is not possible to access the Internet if there is no fixed or mobile telecom/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 natural 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;

---

<sup>75</sup> ITU World Telecommunication/ICT Indicators database, available at <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx> (accessed 22 February 2019).

<sup>76</sup> Statista, available at [www.statista.com](http://www.statista.com) (accessed 22 February 2019).

- consultation of medical databases;
- 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. Likewise, 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).

#### 8.1.4. Social networks

Social networks, like 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. 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 (ibid.).

#### 8.1.5. 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;<sup>77</sup> 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.

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, and therefore in many emergency situations becomes the first and often only link when other systems fail.
- 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.

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 can be used for medium- and long-range communications, fulfilling the function of storage and retransmission. Many different communication modes are used by radio amateurs, including radiotelegraphy through Morse code, especially when basic equipment is used or the transmitter is of low power; data communication; links in the HF band (short wave); packet radio communications; radiotelephony, i.e. voice radio links; frequency modulation, which offers high sound quality; and communication of images.

Finally, 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 communications. The normal role of the amateur radio service is to establish and support communications for those who directly carry out emergency operations.

---

<sup>77</sup> 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](http://www.iaru.org/uploads/1/3/0/7/13073366/ifrcandiarumou.pdf) (accessed 22 February 2019).

#### 8.1.6. 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 among the different means of communication discussed in this chapter.

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 must 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 must 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 discussed in this chapter, 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 natural 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.

#### 8.2. Vulnerability and risk analysis of telecom/ICT networks

The government must maintain and update a map of risks and vulnerabilities of the telecom/ICT networks, taking into account the different types of disasters that may affect different regions of the country. It is essential to know which networks are at risk of collapse and to take appropriate measures in advance to ensure communications in the event of a natural disaster.

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

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 on the networks of the different telecom/ICT services. This database should include the capacity of the networks and their possible expansion in case of an emergency.

#### 8.2.1. Telecom/ICT database for emergencies

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

- telecom/ICT services available;
- terrestrial coverage;
- location of the specific infrastructure, e.g., towers, power stations, wired networks, etc.;
- vulnerability of the infrastructure to different types of disasters, classifying it, for example, as high-, medium- or low-risk.

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

### 8.3. Early Warning Systems

Telecom/ICTs play a key role during the preparedness phase of disaster management through the deployment of Early Warning Systems (EWSs). Providing timely information to the population by means of telecom/ICT networks for monitoring, early warning and alerting is critical to reducing the impact of disasters and saving lives.

EWSs include four elements. Failure in any one of these elements can mean failure of the whole system (UNISDR, 2006a):

- Risk awareness: Systematically collect data and undertake risk assessments: Potential hazards and vulnerabilities, as well as their patterns and trends, need to be well known. Developing risk maps and collecting as much data as is available is helpful in risk assessment.
- Monitoring and warning services: Develop hazard monitoring and early warning services. Based on the risk assessment, key parameters related to a specific hazard should be monitored, and accurate and timely warnings should be developed and tested.
- Dissemination and communication: Communicate information about risks and early warnings. EWS must reach the entire at-risk population. In addition, those receiving communications must understand the risks involved and the warning information.
- Response capability: Build national and community response capabilities. Response plans should be up to date and tested, and the population should be prepared and ready to react to warnings.

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 are 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. However, warnings, alerts, and observations made on the ground, i.e. by terrestrial means, are usually more precise than satellite observations. Nevertheless, satellite observations are useful when terrestrial options do not exist or have been disabled by disasters.<sup>78</sup> Thus, a comprehensive EWS strategy should use both terrestrial and satellite services to monitor possible disasters and provide accurate and timely warnings and alerts.

EWSs can be provided through the different telecom/ICT services described above. 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 EWS, based on sirens or public address systems connected to sensors that trigger an alarm when a specific threshold is reached, can also be developed.

Broadcast 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).

**Box 8. Case study: Butaleja district in Eastern Uganda – Flood Early Warning Systems<sup>79</sup>**

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:

1. A sensor placed in the river;
2. A solar-powered siren adjacent to the river; and
3. 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

<sup>78</sup> 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.

<sup>79</sup> ITU (N.D.).

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.

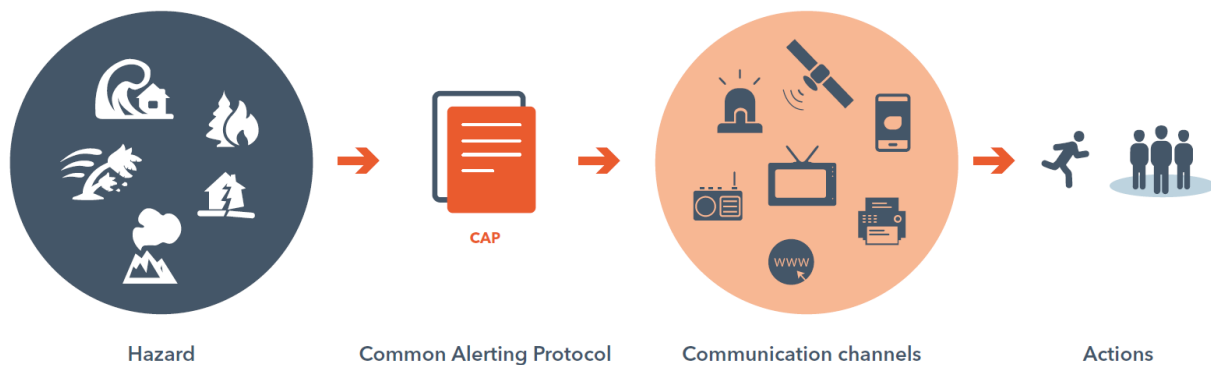
**Figure 10: Ugandan Flood Early Warning Systems**



#### 8.4. 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 11: Common Alerting Protocol**



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. Those alerting area data allow all manner of telecom/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 telecom/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. For example, the United States National Weather Service publishes a CAP news feed for each “forecast zone”. These several thousand CAP news feeds are also aggregated as one feed into a United States Federal CAP news feed. That United States Federal CAP includes more than 1 000 other CAP news feeds, published by states and cities. In turn, that United States national feed is one among 80+ national news feeds that are already part of a prototype global-scale Alert Hub.<sup>80</sup>

Today, 75 per cent of the world’s people live in nations that already have, or are currently developing, official, national-scale news feeds with public CAP alerts. However, uptake is uneven, and it is slowest among developing countries. All manner of organizations are challenged to work toward a future when societies everywhere can fully benefit from CAP-enabled alerting.

#### **Box 9. Case study: Common Alerting Protocol<sup>81</sup>**

The Integrated Public Alert and Warning System programme (IPAWS), established in the United States 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

<sup>80</sup> Alert Hub, available at <http://alert-hub.org> (accessed 22 February 2019).

<sup>81</sup> National Council on Disability (2014).

many different communications systems”.<sup>82</sup> CAP allows for messages to include content such as photographs, maps and streaming video. This system operates in multiple languages and provides information in both text and audio formats.

Other countries besides the United States have deployed this technology in order to develop a more inclusive alert system. 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.<sup>83</sup>

China, on the other hand, implemented CAP-enabled alerting for all hazards nationwide. In particular, its 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 Australian, 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, people 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.<sup>84</sup>



#### Recommendation 6:

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

<sup>82</sup> Ibid.

<sup>83</sup> Government of Canada, Canadian profile of the CAP-CP, available at [www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdncs/capcp/index-en.aspx](http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdncs/capcp/index-en.aspx) (accessed 22 February 2019).

<sup>84</sup> 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](http://www.bom.gov.au/metadata/CAP-AU/About.shtml) (accessed 22 February 2019).





#### Recommendation 7:

Early Warning Systems should be designed and deployed, linking all hazard-based systems when possible to take advantage of economies of scale and enhance sustainability and efficiency through a multipurpose framework that considers multiple potential hazards and end-user needs. An inventory of such systems should be included in the NETP and periodically reviewed and updated.

## 9. Development of capacities and drills

Preparing for management of an emergency requires continuous training and capacity-building efforts for both the administrators leading emergency responses and the wider community. The development of capacities 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, 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 must 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, telecom/ICT network infrastructure and other areas identified throughout the planning process.

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

- identifying best practices in existing programmes and developing SOPs and other guidance that responds 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 should encompass multiple subjects, from basic aspects of the use of telecommunications during emergencies to technical concepts. Trainings 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”), this practice is not sufficient in the case of emergency telecommunications. Implementing periodic trainings also builds staff familiarity with their additional responsibilities during an emergency event and allows them to familiarize themselves with some of the potential challenges that could arise (ITU, 2001).

Frequent 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 (ibid.).

Likewise, such training activities provide an opportunity to confirm the availability and reliability of emergency equipment that is not frequently used. Trainings 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 (ibid.).

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 must be spent reviewing the deficiencies encountered and the mistakes made, so that the lessons learned can be 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 (ibid.).

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

In addition, it is widely acknowledged that disaster response depends on teamwork. Therefore, it is important that training exercises include all potential 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, among others, are as follows (ibid.):

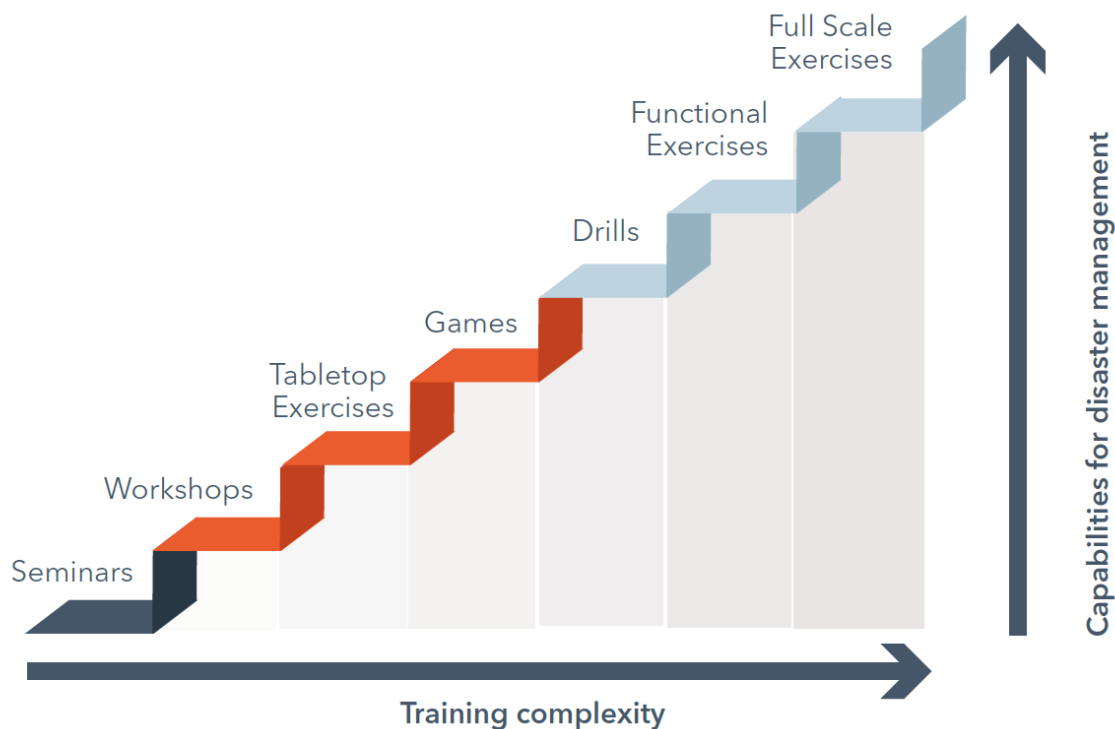
- Develop training and exercise programmes that target gaps in emergency communications capabilities and use new technologies.
- Identify opportunities to integrate more private and public sector communications stakeholders into training and exercises.
- Use regional governance structures to develop 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.

### 9.1. Drills and simulations in practice

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

- TTX refers to a facilitated discussion of a simulated emergency, generally conducted in a low-stress environment with participants seated around a table. Drills, on the other hand, are activities in which specific operations, functions or systems are repeatedly tested in a supervised setting.
- A drill, different from other types of training, 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 TTX.
- 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.

**Figure 12: Training**



In the case of telecommunication drills and simulations, exercises should include as many different actors 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 telecoms 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.

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 TTX and drills to full-scale need 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 a debrief, in which the participants and facilitators of the exercise share their experiences and challenges they 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 10. Case Study: NetHope<sup>85</sup>**

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 NetHope's 56 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 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.

<sup>85</sup> NetHope (2018), *Planning a disaster: detail and expertise required for disaster preparation training*.

**Box 11. Case study: gear.UP<sup>86</sup>**

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 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.

In particular, this exercise involves an intensive seven-day field simulation held annually and led by WFP as global leader of ETC and the Logistics Cluster. In the field, the exercise tests, among other things, IT and telecoms, 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<sup>87</sup> 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.

**Box 12. Case study: Earthquake drills<sup>88</sup>**

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.

---

<sup>86</sup> Emergency Telecommunications Cluster, OpEx Bravo and LRT (gear.UP), available at [www.etcluster.org/training/opex-bravo-lrt](http://www.etcluster.org/training/opex-bravo-lrt) (accessed 22 February 2019).

<sup>87</sup> 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](http://www1.wfp.org/FITTEST) and [www.etcluster.org/content/wfp-fittest-training-services](http://www.etcluster.org/content/wfp-fittest-training-services), both accessed 22 February 2019.)

<sup>88</sup> World Bank (2016), *Learning from disaster simulation drills in Japan*.



**Recommendation 8:**

The NETP must include a mechanism for enhancing training and capacity building for both the administrators leading emergency responses and the wider community using telecom/ICT. 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 existing procedures and policies.

## 10. Support for people with specific needs

Disasters are especially difficult for vulnerable people, such as people with disabilities, children, the elderly, migrant workers, the unemployed, people with lack of connectivity skills and persons displaced from their homes due to previous disasters, among others. Therefore, it is important to ensure that disaster management plans understand and respond to their needs. The following are 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 telecom/ICT are considered during any project on telecom/ICT-based disaster management processes or telecom/ICT-based development projects.
- Use multiple strategies and mechanisms to promote accessible telecom/ICT, including legislation, policy, regulation, license requirements, codes of conduct and monetary or other incentives.
- Build the capacity of vulnerable populations to use telecom/ICT 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 telecom/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.

### 10.1. Telecom/ICT to support people with specific needs during emergency events

The use of several different types of telecom/ICT can be vital for supporting people with specific needs, including those with disabilities during emergencies, considering the different difficulties that could arise according to the type of disability. For example, blind people cannot see, but they can hear; paralyzed people can hear and see, but they cannot run. 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 telecom/ICT and take into account all possible needs that every person might have.

Telecom/ICT can be a key tool in disaster response and management operations, providing the possibility to use multiple modes and channels to reach traditionally marginalized or especially vulnerable groups before, during and after a disaster. Apart from traditional forms of telecom/ICT (TV and radio), the world of telecom/ICT 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 (ibid.).

However, while the content for disaster preparedness and planning materials can be created and delivered in multiple formats through multiple media, many of these formats may be inaccessible to people with disabilities. 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. Examples of the incorporation of multiple forms of telecom/ICT into the dissemination of warning alerts, which is key to bringing messages to marginalized communities, are specified below (ibid.):

- 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 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 JavaScript, and those on older browsers. The Emergency 2.0 Wiki Accessibility Toolkit<sup>21</sup> 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.

- **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) (ibid.).

### **Box 13. Case study: PLUSVoice<sup>89</sup>**

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. In particular, 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.

<sup>89</sup> Qureshi (2012), *Accessible ICT tools and services in disaster and emergency preparation*.

This company's 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 (ibid.).

**Box 14. Case study: Wireless Emergency Alerts<sup>90</sup>**

Wireless Emergency Alerts (WEA) is an alert network that operates in the United States with the purpose of disseminating emergency alerts to mobile devices. This system allows geographically targeted alerts and warnings in the form of text-like messages that are broadcasted 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.<sup>91</sup>

**Box 15. Case study: Get Ready Get Through<sup>92</sup>**

The Government of New Zealand created a website called Get Ready Get Through,<sup>93</sup> 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 on short notice.<sup>94</sup>

<sup>90</sup> National Council on Disability (2014).

<sup>91</sup> United States Federal Communications Commission. Wireless Emergency Alerts Consumer Guide. Available at [www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea](http://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea) (accessed 22 February 2019).

<sup>92</sup> Qureshi (2012).

<sup>93</sup> Get Ready Get Through, available at [www.getthru.govt.nz/](http://www.getthru.govt.nz/) (accessed 22 February 2019).

<sup>94</sup> Ibid.



### Recommendation 9:

The NETP should include multiple forms of telecom/ICT for the dissemination of warning alerts, which are key to bringing messages to all the people, including those with specific needs, and marginalized communities. It is important to ensure that the NETP understands and responds to everyone's needs.

## 11. NETP: Step by step

This chapter provides a step-by-step guide for building an NETP. The first section of the chapter describes the topics that must be included in the NETP. The second section of this chapter describes each of these topics. The third and last section presents a step-by-step process to draft the NETP. It is important to note that, in drafting the NETP, the information provided in the chapters of these guidelines should be considered jointly with this last chapter.

### 11.1. Topics to be included in the NETP

In the ITU proposal, the NETP is composed of five main sections. The first section is a general introduction to the NETP and the remaining four sections address the different phases of disaster management that have been described in the preceding chapters of these guidelines. Each of these sections must be based on the specific characteristics of each country. Note that modifications can be made to these sections based on the specific needs of the country and the preference of the author who is developing the NETP. However, it is important to make sure that all the topics described below are considered.

- I. General Introduction:
  - (a) Purpose and scope of the NETP and coordination with the national disaster risk management plan;
  - (b) Description of the phases of disaster management and how telecom/ICT services can be used to support all activities of disaster management;
  - (c) Telecom/ICT operators/ service providers, facilities availability and service penetration;
  - (d) Treaties and international cooperation agreements.
  
- II. Mitigation phase:
  - (a) Map of the type of hazards the country faces;
  - (b) Risk analysis of critical telecom/ICT networks;
  - (c) Reducing the vulnerability and improving the resilience of telecom/ICT networks;
  - (d) Legal and regulatory framework to support emergency telecom/ICT services.

- III. Preparedness phase:
  - (a) Standard operating procedures;
  - (b) Response and contingency plans;
  - (c) Telecom/ICT networks for monitoring, early warning and alert systems;
  - (d) Telecom/ICT and broadcasting to raise awareness;
  - (e) Cooperation with different stakeholders, including operators and private sector;
  - (f) Training and exercises;
  - (g) Support for vulnerable people.
  
- IV. Response phase:
  - (a) Communication and coordination between first responders and different 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) Connecting families and friends, enabling call centres, etc.
  
- V. Recovery phase:
  - (a) Damage and needs assessment;
  - (b) Rebuilding and improving telecom/ICT infrastructure;
  - (c) Incorporating redundancy into telecom/ICT networks;
  - (d) Identifying locations in need of recovery assistance, tracking recovery activities;
  - (e) Coordinating reconstruction activities.

## 11.2. Drafting the NETP

### 11.2.1. General introduction

This first section of the NETP defines the purpose and scope of the NETP, which is generally to promote and facilitate communication and information sharing about threats and hazards 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. In summary, the NETP describes how telecom/ICT services will be used to help prepare for and respond to disasters.

The purpose and scope of the NETP should be in line with existing legislation 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 management addressed in the plan, and describe how telecom/ICT services can be used to support these phases.

In this section, the NETP must include a description and inventory of the commercial, private and government telecom/ICT operators and networks available for use in a disaster event. It must also include the penetration levels of these services and map the infrastructure and services offered across the country, identifying those regions where there is a lack of telecom/ICT services.

The NETP should also reference any treaties or international cooperation agreements the country has signed related to telecom/ICT service cooperation for disaster relief, such as the Tampere Convention, or any partnerships with the private sector. Since an NETP is dynamic, any new treaty, cooperation agreement or private partnership should be subsequently included in the NETP.

#### 11.2.2. Mitigation phase

As mentioned before, this phase aims to minimize the adverse impacts of hazardous events. The types of disasters are unique to each country. Therefore, the NETP must include a hazard profile of how and where the country is vulnerable. Geographic maps depicting the likely locations of different types of possible disaster are useful. This is critical for the analysis of telecom/ICT infrastructure risks and contingency plans, as well as for determining the type of warning systems needed. Risk analysis of critical telecom/ICT infrastructure is key to reducing the vulnerability and improving the resilience of telecom/ICT networks. This analysis must take into consideration the specific risk disaster map and hazard profile mentioned above, and the description and inventory of telecom/ICT networks.

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

Finally, the NETP must describe the existing legal and regulatory framework related to telecom/ICT services for emergency situations. If no framework is in place, it is necessary to draft a framework that supports the NETP and which provides for enforceable authority for a government entity to, for example, request telecom/ICT infrastructure deployment from operators. As previously discussed, laws and regulations determine coordination mechanisms, allocation of funds, communication channels, SOPs and identification of decision-makers at different agencies. If there is a legal and regulatory framework in place, it is necessary to analyse if it includes all the necessary provisions for the efficient and effective development of an NETP.

#### 11.2.3. Preparedness phase

Developing the NETP is part of the preparedness phase. The NETP must include detailed plans and procedures, as well as the protocols for coordination and communication of those involved in emergency management. 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 multistakeholder community when a disaster strikes.

The NETP must include the functions, responsibilities and contact points, as well as contact details (e.g. e-mail or phone number), for each government agency and stakeholder related to telecom/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 must also be drafted and included in the NETP to establish arrangements in advance to enable timely, effective and appropriate responses to disasters. Inputs to draft response and contingency plans should be based on the typology of disaster analysis, and must include the lack of telecom/ICT infrastructure in vulnerable regions.

Early warning and alerting systems should be deployed during the preparedness phase. In addition, an inventory of existing monitoring early warning and alerting systems must also be included in the NETP. Information regarding the location, coverage and technology used by the system, as well as the type of hazard the system was developed for, must be included in the NETP for each early warning and alerting system. This section should also address administrative aspects of EWS, such as who is responsible for maintenance and operation of the system. Similar to telecom/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, appropriate for the type of disaster likely to occur, and whether the systems are well maintained and in working condition.

The NETP should also include guidelines for training, drills and mock exercises. 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 are key to increasing resilience, reducing risks and limiting fatalities and economic losses of the population. Telecom/ICT and broadcasting services are important tools for carrying out this awareness and education. Regulations should be in place that allow the government to use such networks to educate the public and increase awareness. The NETP must include these regulations, e.g. requiring broadcasters and mobile operators to support communication and messaging strategies to the affected population before and during emergency situations.

#### 11.2.4. Response phase

During this phase, the plans and procedures established in the preparedness phase are executed. Emergency telecom/ICT availability must be coordinated among all stakeholders during this phase through the defined contact points. This is especially important considering that the need for interoperable and continuous communications capabilities for all responders is particularly urgent during the response phase of disasters. Therefore, during this phase, the country level coordinator

or the lead government agency, working together with information managers and partners, should ensure that communications processes, partnerships and resources are effectively synchronized and utilized during response operations.

The NETP must incorporate procedures for obtaining information on existing telecom/ICT capacities that could be made available for continued emergency disaster response. This should include, at a minimum, the following:

- Damaged infrastructure and services assessment (government and commercial/public networks):
  - (a) mobile and radio systems;
  - (b) emergency dispatch services;
  - (c) status of terrestrial systems/public mobile systems;
  - (d) broadcast radio/TV stations;
  - (e) in-country VSAT provider availability;
  - (f) pre-positioned emergency MSS equipment;
  - (g) Internet services;
- Establishment of emergency connectivity;
- Maintenance and reestablishment of government networks;
- Maintenance and reestablishment of commercial/public networks.

#### 11.2.5. Recovery phase

The recovery phase focuses on providing the help needed for the community to return to pre-emergency levels of safety and functionality. During this phase, it is especially important that stakeholders work to restore damaged telecom/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.

The rebuilding and improvement of telecom/ICT network infrastructure must also include network deployments so as to prepare for future disasters. In addition, government and the private sector should take advantage of the opportunity to rebuild telecom/ICT infrastructure to deploy new technologies that are more efficient and less expensive.

Finally, telecom/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 logistical arrangements, including ICT needs, for example, or information management requirements.<sup>95</sup>

---

<sup>95</sup> For more detail, see European Commission, United Nations Development Group and World Bank (2013).

### 11.3. NETP drafting process

During the drafting of the NETP, it is important to include the views and opinions of all 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.

- I. Government:
  - Advisors to the Head of State (or Head of Government if possible);
  - If there is existing legislation/regulation, 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 office;
  - Ministry of communications (telecom policy);
  - Telecom regulatory authority (telecom regulation);
  - The entity responsible for spectrum policy/allocation (could be one of the above or an independent body);
  - First responders: police, firefighters, civil defence, etc.;
  - International organizations such as the Red Cross (organizations present in the country).
  
- II. Public telecom/ICT/media providers (voice, data–Internet, TV, radio, etc.):
  - Mobile cellular service providers;
  - Fixed telephony providers;
  - Satellite providers;
  - Broadcasters (TV and radio);
  - Others present in the country.
  
- III. Private networks
  - Amateur radio;
  - Private mobile network providers (e.g. trunking networks);
  - Others (depends on what desk research reveals for a given country).
  
- IV. International organizations, such as:
  - ITU;
  - OCHA;
  - UNISDR.



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.

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

- Step 1: Conduct desk research to collect and analyse information regarding the high-level government statements, policies and regulation on telecom/ICT for disaster management (see Chapters 6 and 8).
- Step 2: Conduct desk research on historical disaster events, hazard profiles (see Chapter 3), existing early warning and alerting systems, telecom/ICT networks and services currently deployed (see Chapter 7).
- Step 3: Hold a workshop to (a) present the overall strategy to draft the NETP; (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 must be invited to the workshop.
- Step 4: Hold private meetings with each stakeholder to further discuss specific sections of the NETP, e.g. telecom/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 SOPs, with the above inputs and following the guidelines set forth in this document.
- Step 6: Hold a second workshop to present the draft NETP based on the inputs of steps 3 and 4. 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 allow 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, or 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 occur.

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

## Annex A – Emergency communications checklist<sup>96</sup>

I. Preparedness
<p><b>a) Administration and responsibility setting</b></p> <p>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.</p> <p><b><i>Government roles and responsibilities</i></b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> What government agency/ministry is responsible for disaster management and response overall in the country?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> How is telecom/ICT prioritized or addressed within the country’s disaster management framework?</li> <li><input type="checkbox"/> How is disaster response management responsibility or authority managed between central government and local or provincial/state governments?</li> </ul>

<sup>96</sup> ITU (2017a).

**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.

- 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.

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.<sup>97</sup>

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 telecom/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?

<sup>97</sup> United States Department of Homeland Security, available at [www.ready.gov/business/testing/exercises](http://www.ready.gov/business/testing/exercises) (accessed 23 February 2019).

- 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?

**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).
- 
- 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 telecom/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.
- 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 (telecom/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.

**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.

***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.

***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?

## 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](http://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](http://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](http://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](http://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](http://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](http://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](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.

Tampere Convention (1998). Available at [www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere\\_Convention/Tampere\\_convention.pdf](http://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 (2015a). Sendai Framework for disaster risk reduction 2015–2030. Available from [www.unisdr.org/we/coordinate/sendai-framework](http://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 at [www.dhs.gov/sites/default/files/publications/Writing%20Guide%20for%20Standard%20Operating%20Procedures\\_0.pdf](http://www.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.