ITUPublications

International Telecommunication Union
Development Sector

National emergency telecommunication plan (NETP)

Model framework for West Africa

National emergency telecommunication plan (NETP)

Model framework for West Africa

Disclaimer

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the International Telecommunication Union (ITU) or of the ITU secretariat concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.

The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or its membership.

ISBN

978-92-61-42371-1 (Electronic version)
978-92-61-42381-0 (EPUB version)

This report was prepared by the International Telecommunication Union (ITU).

Please consider the environment before printing this report.

Foreword

I am pleased to present a national emergency telecommunication plan model framework for countries in West Africa. This model outlines strategies and frameworks for the effective use of information and communication technologies (ICTs) throughout the disaster management cycle to significantly enhance preparedness and resilience. It aims to ensure coordination across all levels of government, with the engagement of the private sector and communities at risk, to reduce vulnerability to a wide range of disasters and natural hazards, including floods, droughts, coastal erosion, storm surges, epidemics, desertification, heatwaves, and, in some areas, landslides and seismic activity. It further provides step-by-step guidance on how to develop legislation, emergency telecommunication regulations, institutional structures, and coordination mechanisms for Member States in West Africa, offering practical recommendations and actionable measures to support countries in building and strengthening their national systems.

Building on this foundation, the model further identifies priority actions to enhance regional and international cooperation, reduce vulnerabilities, strengthen the resilience of telecommunication infrastructure, and advance the development of robust early warning systems across the region. This model complements the existing framework for Southern African Development Community (SADC) countries, which was developed in 2024, and is now in the process of regional implementation.

I am confident that, through the use of this model, countries in West Africa will be better equipped to prepare for and respond to disasters by establishing effective frameworks for the deployment of emergency telecommunications across all phases of disaster risk management, guided by a comprehensive and forward-looking strategy for disaster risk reduction and resilience.

Dr Cosmas Luckyson Zavazava
Director of the Telecommunication Development Bureau
International Telecommunication Union

Table of contents

List of figures and tables

Figures

Tables

Acronyms

CAP	common alerting protocol
CB	cell broadcast
DMP	disaster management policy
DRM	disaster risk management
ETC	Emergency Telecommunications Cluster
EWS	early warning system
EW4All	Early Warnings for All Initiative
GMDSS	Global Maritime Distress and Safety System
ITU	International Telecommunication Union
MHEWS	Multi-hazard early warning system
NEMA	National Emergency Management Agency
NEMO	National Emergency Management Organization
NETP	national emergency telecommunication plan
NGOs	non-governmental organizations
SOP	standard operating procedure
ICTs	information and communication technologies
UNDP	United Nations Development Programme
VHF	very high frequency
VSAT	very small aperture terminal

1 Introduction

The International Telecommunication Union (ITU) has developed guidelines for creating plans that enable nation-States to develop policies, procedures and governance frameworks facilitating reliable and resilient communications[1]. A *national emergency telecommunication plan* (NETP) sets out the strategy to enable and ensure communications availability during the mitigation, preparedness, response, and recovery phases of disaster risk management (DRM). This is achieved by promoting coordination across all levels of government, between public and private organizations, and within communities at risk.

This NETP document considers the definition of policies, the structure, and the methods of coordination between the different actors during all four phases of DRM (mitigation, preparedness, response, and recovery) and is intended to form a template such that the countries listed in Table 1 below can develop their own detailed, individual, NETP documents customised to their unique circumstances in so far as they relate to or depend on telecommunications and information and communication technologies (telecommunications/ICTs). A completed, country specific, NETP document also establishes the principles that guide the allocation of resources and responsibilities for the achievement of the proposed objectives, including the expected telecommunication/ICT response times, tasks, and processes.

Table 1: List of countries in-scope of this document

Benin	**Liberia**
Burkina Faso	**Mali**
Cape Verde	**Mauritania**
Gambia	**Niger**
Ghana	**Nigeria**
Guinea	**Senegal**
Guinea-Bissau	**Sierra Leone**
Ivory Coast	**Togo**

The NETP has a transversal nature given the importance of telecommunications/ICTs during DRM. Therefore, it must be carried out under the leadership of the national government, must be an integral part of the country's national disaster plan, and must be based on the nationwide structure and governance model established for risk management of disasters.

The following sections address these points and propose a series of action items that should be completed to enhance and update the telecommunication/ICT plan for DRM in each country. As this is a framework document, there are generic sections in the main body of the document which will need to be customised with data specific to each country concerned. Country specific reference data is included in the Appendix to this document and should be used to populate the relevant sections to create the country specific NETP.

[1] ITU Guidelines for national emergency telecommunication plans

Objective and scope of the NETP

A completed NETP document describes the relevant elements of telecommunication/ICT use for DRM that a country relies upon during the four phases of DRM: mitigation, preparedness, response, and recovery. This refers to ***national emergencies*** and the management of ***national disasters***, rather than matters concerning minor incidents and similar events – although there will clearly be some relationship between the two, for example where the ability to communicate with emergency services such as Fire, Rescue, Police or Ambulance/Paramedic services are concerned. Particularly, the purpose of this document is to guide the development of an NETP tailored for the specific needs of one of the "in-scope" countries listed in Table 1, facilitating the creation of their own individual NETP document and guiding how telecommunications /ICTs support national emergencies and associated disasters. Once completed, an NETP defines the actions of the telecommunication/ICT sector to provide support for and improve coordination between the different agents involved in DRM within each country. In so doing, an NETP also seeks to strengthen telecommunications/ICTs so that the relevant actors in this sector can appropriately support efforts to mitigate disaster risk, as well as to prepare, respond and recover in the face of future emergencies.

This document is intended for all persons and institutions involved in DRM within the in-scope countries who will have responsibility for developing and implementing an NETP tailored to their own country's specific needs. This includes authorities at all levels of government, technical institutions, the private sector, and other actors in the telecommunication/ICT sector, as well as in the and emergency humanitarian sectors.

Structure of a completed NETP and this framework document

This document follows the generic structure of an NETP document and is divided into 22 sections. Sections 2 to 7 discuss the institutional and normative framework for emergency telecommunications/ICTs and in a completed NETP document would describe the pertinent legislation that sets out how DRM is managed within the country in question, along with identifying the roles, responsibilities, policies, regulations and entities and agencies involved. Sections 8 to 22 set out to the main components that should be considered in each of the four phases of DRM (mitigate, prepare, respond and recover), and delineate some recommendations and key action items to be carried out to continue developing and updating an effective NETP. Sections 8 to 12 correspond to the mitigation phase of DRM and deal with topics such as vulnerability to natural and technological hazards, the current state of the telecommunication/ICT sector, and the establishment of a specific telecommunication/ICT regulatory framework for disaster risk management. Sections 13 to 17 correspond to the preparedness phase and includes topics regarding telecommunication/ICT standard operating procedures, contingency planning, and early warning systems. The response phase is covered in sections 18 to 20. These sections describe topics such as communication and coordination during emergency response, collection and analysis of information, and emergency awareness and updates. Finally, the recovery phase for DRM is addressed in sections 21 and 22 which present topics such as the assessment of damage of the telecommunication/ICT infrastructure, and the reconstruction and follow up activities to be carried out after the disaster. To create an NETP, this template should be updated with the relevant country specific information in each of the sections, some of which are included in appendices.

Summary of action items

The following list the action items identified in the rest of this document and are provided here as an action summary. As this is a framework and template for the development of an actual NETP, it is expected that these action items should be addressed within the calendar year that the first NETP for a country is developed and after this, the NETP should be reviewed and updated with as many items addressed as possible, so the focus can then move on to refining the scope, breadth, and detail of the NETP as a subsequent activity.

Action Item 1: Development of legislation for DRM

Legislation for disaster risk management should be documented in the NETP and if it does not exist then it should be created, made official, easily accessible, and maintained. Ideally this should be on-line and maintained such that when any of the different elements are added to or updated, the changes and additions are reflected in the other elements. For example, relevant legislation should consider referring to the Tampere Convention, if the country has acceded to it and if not, serious consideration should be given to incorporating its provisions and ensuring they are implemented and communicated to all stakeholders so they can embrace them in their DRM plans.

Action Item 2: Maintenance of national disaster management plan

A national disaster management plan should be created, if one does not already exist, this should be updated and published, and the most recent version should be made accessible, based on the legislation for disaster risk management currently in force. The authorities in charge of disaster risk management in the country should incorporate the Tampere Convention's provisions in the Disaster Management Plan if necessary, making the necessary regulatory adjustments, complementing the current regulations on international assistance for disaster risk management. These, and any necessary further steps, will help all those involved in disaster risk management to internalize and effectively adopt this legal framework for cooperation and embed it the operations and practises of all relevant stakeholders.

It should include up-to-date information regarding coordination between relevant actors involved in DRM, as well as the emergency response communications network and the necessary telecommunications equipment and services, among other elements, identified by the NETP and show greater alignment with any prevailing comprehensive disaster management plan or policy within the nation-State concerned.

Action Item 3: Integration of plans and policies

Ensure the responsible agencies, government departments and other entities involved with comprehensive disaster risk management and associated telecommunications/ICTs within the country are appropriately identified including any inter-relationships, shared or devolved responsibilities.

Action Item 4: Integration of plans and policies

The development plan should set out a general policy calling for the support for proposals that facilitate communication during emergencies. There should be a link to the national disaster plan, reference to the comprehensive disaster management policy, and this national emergency

telecommunication plan as proposals are developed and considered, to ensure they are up to date, consistent and aligned. A key goal should be to drive the extension and availability of telecommunication infrastructure to support development aims in general and specifically ensuring telecommunications/ICTs can be exploited to the maximal extent in the four phases of emergency preparedness and response. This must address how telecommunication/ICT infrastructure can improve early warning detection of hazard alerts and the dissemination and communication of alerting information to all parts of the population, including any marginalized groups.

Action Item 5: Creating and maintaining hazard maps

Maintaining and ensuring hazard maps for the different types of hazards exist is an essential contributor to disaster planning and the development of mitigation strategies. Information must be detailed at the municipal level and should be available to telecommunication/ICT operators to ensure they consider these factors in infrastructure planning and resilience. Also, it should include information on the most vulnerable communities, specifying the type of hazards they are prone to, as well as the communications resources available in each of them. This activity could be carried out with the support of the responsible authorities and relevant planning departments and go beyond the practise of collating Geographic Information System (GIS) data to become proactive curation of this data, identifying gaps and driving project requirements to expand and maintain GIS/hazard map information.

Action Item 6: Service provider supporting policies and procedures

The public network service operators should be asked to provide details of their business continuity and disaster management processes and procedures. This activity could be carried by the telecommunication regulator with support of any government department responsible for disaster management. This should also include any relevant planning departments to ensure alignment.

Action Item 7: Early warning capabilities

Support for early warning capabilities should be established from the point of view of both hazard detection and dissemination of alerting information to as wide a range of communications channels as possible; including the role that service providers can fulfil. It is essential that whatever combination of solutions are deployed, that they deliver timely, accurate and actionable information to all population groups. The use of standard based protocols, such as the common alerting protocol (CAP), should be assessed to maximize interoperability between service providers and between the government department responsible for disaster management and each service provider. This should also solicit information on the mechanisms supported that enable national coverage and localisation of alert messages, such as cell broadcast and location-based SMS and identify any constraints associated with these. This should also include consideration of any indication concerning 2G/3G closure and migration to 5G radio and any impact on early warning that may result from that, including the impact on monitoring devices/ equipment and the gathering and dissemination of warning information.

Once these aspects have been confirmed, this NETP should be updated with the information obtained.

Action Item 8: Emergency communications network

Where an emergency communications network (ECN) is implemented, coverage maps for the entire nation need to be established and any gaps identified that could limit coverage in an emergency scenario. Furthermore, spectrum licensing should ensure the ECN uses dedicated radio bands that are protected for this purpose. Consideration should also be given to the interconnection of this system with the fixed and mobile networks operating to ensure ease of use across all areas of the country. Furthermore, the ECN should be assessed in the context of command and control for Early Warnings for All Initiative alert communications.

Action Item 9: Network inventory and coverage

Update the network inventory and coverage of mobile and fixed telecommunication/ICT operators, and radio and television broadcasting. Also, maintain an updated database with the focal points in charge of technical aspects as well as with those in charge of communication of alerts and relevant information regarding disasters as part of the dissemination and communication aspects of achieving early warning for all. Include network information and coverage of radio amateurs and first responders (police, firefighters, etc.) and identify any gaps. Assess the implementation of other options on telecommunication/ICT infrastructure, such as satellite services, including satellite devices for voice/broadband communications and consider the possibility of community WiFi to strengthen emergency response and recovery activities.

Action Item 10: Vulnerability analysis

All telecommunication/ICT service operators, mobile, fixed, and radio and television broadcasting operators, as well as government networks, in conjunction with the relevant regulatory body, should develop (or update) and present for approval to the government agency responsible for disaster management a vulnerability analysis of the critical infrastructure of their networks, including an inventory of the infrastructure, and power, maintenance and connectivity evaluations along with consideration of the risks associated with cyber security or other technological factors. This should also consider how the telecommunication/ICT services will participate in a national early warning for all solution.

Action Item 11: Alignment and development of regional regulations

The Government should develop specific regulations for the telecommunication/ICT sector regarding disaster risk management in the country. This includes establishing specific regulations based on the functions granted by the legislation, for each of the phases of disaster risk management, encouraging telecommunications operators to actively participate in each phase of disaster management.

Action Item 12: International cooperation

The relevant government departments must establish specific regulations for the implementation of the Tampere Convention where that has not already been achieved.

Coordination and collaboration with different international agencies such as the ETC (Emergency Telecommunications Cluster) and ITU (International Telecommunication Union) on issues of prevention and response to eventual disasters or emergencies is imperative.

Action Item 13: Standard operating procedures

1. Develop or update standard operating procedures for emergency and disaster response related to communications within and between agencies and technical means for communication (voice/data), including interoperability.
2. Define the government entities and the contact points (key decision makers) within these entities that must maintain communication during a disaster or emergency.
3. Maintain an updated database with these focal points of every agency, and where appropriate any associated partner organization, countries, or other external entities, involved in disaster management.
4. Analyse the possible interoperability between the equipment (wireless) and the communication networks of the government entities.
5. Establish a set of radio frequencies that can be used for the communications of the contact points (key decision makers) compatible with the radiocommunication equipment being used and ensure it is aligned with any similar activities to ensure regional compatibility.
6. Establish alternative methods of communications, if necessary, for example through existing communication operators.
7. Develop connectivity plans for the satellite equipment available, if that is the case, to be used during a response phase as well as procedures for their use as primary or alternative communications between relevant stakeholders involved in disaster response.

Action Item 14: Contingency planning for public and private networks

Public and private networks, including mobile, fixed and broadcasting operators must keep their contingency plans for an emergency updated. Measures such as network redundancy, mobile base stations, secondary energy sources, among others, must be considered and included in the network design, management, and maintenance plans, especially in those areas at risk according to the hazard maps and risk assessments, and considering the network vulnerability analysis. This is particularly important where there may be areas operated by independent organizations to ensure compliance with State-wide capabilities and compatibility between systems.

Other type of networks, such as satellite networks, should also be considered in the contingency plans, e.g., satellite equipment in safe warehouses, and connectivity plans for their use during the response phase of a disaster.

A process and procedure should be developed by the government agency responsible for disaster management to ensure these contingency plans are created, maintained, and verified that they are compatible with the wider policies and plans administered through that organization.

Action Item 15: Early warning alert message dissemination

The UN executive action plan for the Early Warnings for All Initiative should be consulted and a roadmap created which demonstrates progress against this initiative which is bench marked.

The current common alerting protocol (CAP) Alerting implementation should be examined to assess its efficacy and identify opportunities for expanding its reach to as broad a number of different channels as possible. Any dependencies for downloading applications to mobile devices should be assessed for limitations in scope and coverage.

Specifically, can it propagate alerts to mobile network cell broadcast and/or location-based SMS, TV, public broadcast radio, etc? Consideration should also be given to assessing interoperability

between the systems operated by public service providers and private networks operated in specific designated areas. Enhancements to surveillance and monitoring systems for probable threats prior to the occurrence of disasters and/or emergencies should also be verified. With the cooperation of the telecommunication/ICT service providers, solutions to warn and alert the public could be implemented, i.e., through mobile cell broadcast technology or broadcasting networks (radio and TV). The role of amateur radio should also be reviewed to establish opportunities for further refinement.

Action Item 16: Training and drills

Telecommunication trainings and drills for emergencies should be regularly carried out to improve emergency responders' capacity with communications equipment, as well as to enhance their ability to execute policies, plans and procedures governing the use of communications networks. The telecommunication/ICT sector should actively participate in these drills and exercises, and develop and carry out their own, to effectively implement the NETP.

Action Item 17: Supporting individuals with specific needs

Working together with network operators and telecommunication/ICT service providers, governments and regulators should develop mechanisms to understand the accessibility requirements needed to guarantee that vital digital communication technologies are inclusive and therefore accessible to all persons, including people with disabilities, with specific needs, the elderly, women, and girls, as well as refugees and immigrants. This should be linked to the existing early warning systems in the country so that people receive and understand the alerts for early actions to take place.

Action Item 18: Communications for central co-ordination points

Consider planning for the development of emergency operations centres or communication and coordination command posts to provide critical communications to users in each organization involved during the response phase of a disaster. These positions can be fixed or mobile, local or remote, and could be located in a vehicle or in a shelter, among other possibilities. Maintaining interoperable and continuous communications between command posts and the rest of the stakeholders, especially the focal point for disaster management within the country, shelters and other key locations, is vital for an effective response to the emergency. The network connectivity to shelters needs to be checked to ensure it is reliable, stable and able to cope with expected demands.

Action Item 19: Response phase communications and ICTs

During the response phase, call centres should be established to warn the affected population of new risks, to disseminate updates about the emergency, and to connect affected populations with their relatives. Generally, these call centres can be in shelters, and should use means of communication that do not congest the networks, for example, text messages. To establish these call centres, countries could use satellite networks, that can be easily installed or seek collaboration with telecommunication/ICT operators or international organizations to establish the required telecommunication/ICT infrastructure.

Action Item 20: Restoration and reconstruction

Restoration and reconstruction of the telecommunication/ICT infrastructure should be based on lessons learned and on the principle of building back better. Also, these activities should involve the active participation of the private sector, including fixed, mobile and satellite network and service providers. An essential aspect for consideration must be how the early warning systems can be improved as part of the reconstruction process.

Action Item 21: Continuing development and lessons learned

Based on the experience acquired during the disaster management, a report should be developed after the response and recovery phases identifying lessons learned and including necessary modifications and improvements that should be made to the NETP. The NETP should be updated every two to three years as a minimum and updated more frequently where there are changes in circumstances, legislation and/or regulations and policies.

2 Description of the four phases of disaster management

Disaster risk management (DRM) has two distinct stages: risk management and crisis management. In the first stage, measures are taken to predict and warn of a disaster in advance, as well as to prevent and/or mitigate its damage. These efforts occur under normal or non-emergency circumstances and correspond to the mitigation and preparedness phases. In the second stage, crisis management takes place during emergencies and includes actions such as search and rescue, response coordination, damage assessment, the activation of a policy response, or the mitigation of a secondary disaster.

2.1 Mitigation

The mitigation phase seeks to carry out actions that aim to prevent an emergency, reduce the probability of its occurrence, and limit the negative effects of unavoidable threats. This phase includes activities such as identifying existing hazards and risks, conducting vulnerability assessments, the construction or maintenance of critical telecommunication infrastructure, and the development of written plans and procedures, such as this NETP.

During this phase, the role of telecommunications/ICTs is to help analyse the risk of potential disasters, disseminate information about impending hazards and on how to mitigate their impacts so that hazards do not lead to disasters, identify communities at risk, and to help implement strategies, technologies and processes that can reduce those negative effects. Activities carried out during the mitigation phase include establishing legal and regulatory frameworks that support the use of emergency telecommunications/ICTs, conducting risk analysis of critical telecommunication/ICT infrastructure, taking steps to reduce the vulnerability of telecommunication networks and improve their capacity of recovery, and assess vulnerabilities to develop multi-hazard early warning systems with the appropriate technology for each case. These strategies should be implemented before and after the emergency.[2]

2.2 Preparedness

The preparedness phase includes the planning and preparations necessary to respond to an emergency event. These include the establishment of multi-hazard early warning systems, training, operational processes, and the implementation of those written plans and procedures developed during the mitigation phase.

Telecommunications/ICTs in this phase are essential to facilitate the dissemination of information and alerts so that the public is aware of the actions they must take during an emergency. Likewise, they must facilitate the coordination and communication of those involved in disaster management.

During this phase, it is important to make and implement plans that reduce the likelihood of communications interruptions, to continuously carry out training and drills, and to regularly carry out activities designed to create awareness about impending hazards among those involved, including campaigns in different formats accessible to the entire population regarding potential hazards and the activities that people must carry out during the response phase.

[2] Federal Emergency Management Agency (FEMA), *The Four Phases of Emergency Management*.

2.3 Response

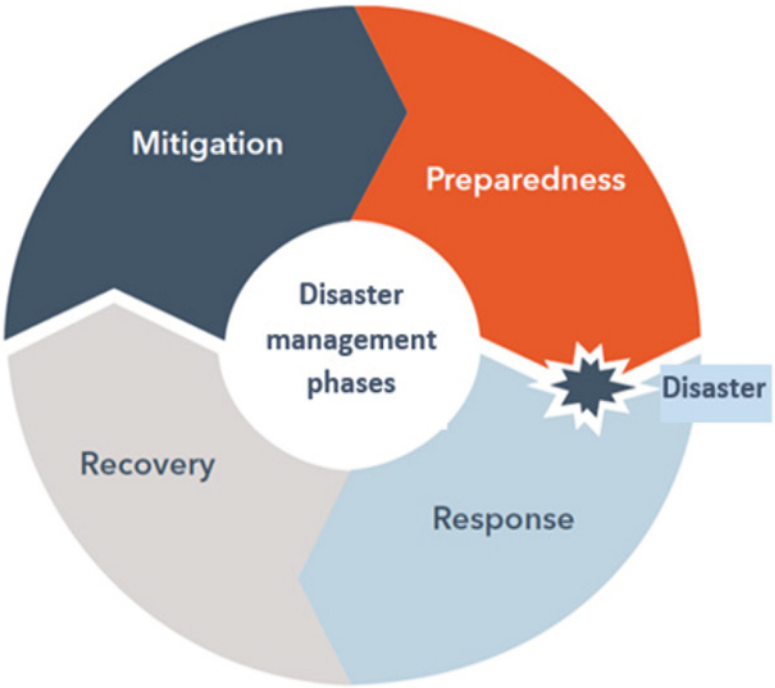
The response phase is carried out during the emergency itself and includes humanitarian activities such as search and rescue, the evacuation of people from affected areas and the opening of shelters, among others.

The role of telecommunications/ICTs during this phase is vital to connect stakeholders such as first responders, government stakeholders and government agencies, communities at risk, shelters, health centres and non-governmental organizations (NGOs), among others. This is especially important considering that several entities carry out a variety of activities and procedures at the local, national, and international level.

2.4 Recovery

The recovery phase runs after a few weeks in the aftermath of disasters and focuses on providing the necessary aid to return to, at least, the initial levels of safety and functionality the community had before the disaster. Activities during this phase include infrastructure reconstruction, restoration of public sector operations, debris removal, among others. This restoration and reconstruction must include telecommunication/ICT infrastructure, especially due to the fundamental role that the sector plays within the community and local economy. The reconstruction should be based in the lessons learned and with the principle of building back better.

Figure 1: Phases of disaster risk management



Source: ITU (2020)

3 Early Warnings for All Initiative (EW4All)

In March 2022, the UN Secretary-General launched the EW4All Initiative, to ensure that everyone on the planet is protected from hazardous weather, water or climate events through early warning systems by the end of 2027.[3] EW4All is co-led by the World Meteorological Organization (WMO) and the United Nations Office for Disaster Risk Reduction (UNDRR), with support from the International Telecommunication Union (ITU) and the International Federation of Red Cross and Red Crescent Societies (IFRC) as well as other partners.[4]

The EW4All initiative considers four key pillars of a multi-hazard early warning system (MHEWS):

1. Disaster risk knowledge and management: Aims to collect data and undertake risk assessments to increase knowledge of hazards and vulnerabilities and trends. It is led by UNDRR with support from WMO.
2. Detection, observations, monitoring, analysis and forecasting of hazards: Seeks to develop hazard monitoring and early warning services. It is led by WMO, with support from UN Development Programme (UNDP), UN Educational, Scientific and Cultural Organization (UNESCO), and UN Environment Programme (UNEP).
3. Dissemination and communication: Focus on communication of risk information so it reaches all those who need it, in an understandable and usable way and using all types of technologies available. It is led by ITU, with support from IFRC, UNDP, and WMO.
4. Preparedness and response: Seek to build national and community response capabilities. Led by IFRC, with support from Risk Informed Early Action Partnership (REAP), Office for the Coordination of Humanitarian Affairs (OCHA), Food and Agriculture Organization (FAO), and World Food Programme (WFP).

In November 2022, an executive action plan was launched to implement this initiative.[5] The plan establishes the different outcomes and activities to carry out in order to effectively implement the initiative in each of the four pillars.

The first pillar focuses on enhancing global risk knowledge and integrating it into inclusive, accessible, and effective early warning systems. This is relevant considering that significant gaps in terms of risk information and assessments persist worldwide, as less than half of the countries with existing early warning systems (EWS) have access to appropriate disaster risk information, and even fewer have national legislation and regulatory frameworks for emergency response. To address this, the executive action plan proposes activities that include the following:[6]

- Significantly strengthen the ability of countries to produce national, sub/national, and local risk information, integrating existing community knowledge, to a defined minimum capability (vulnerability, exposure, hazard).
- Ensure that countries have access to open and relevant risk data, metrics, and analysis to support decision-making.
- Develop institutional capacity to incorporate risk knowledge into early warning systems.

---

3 UNDRR. Early Warnings for All Initiative. Retrieved from: https://www.undrr.org/early-warnings-for-all

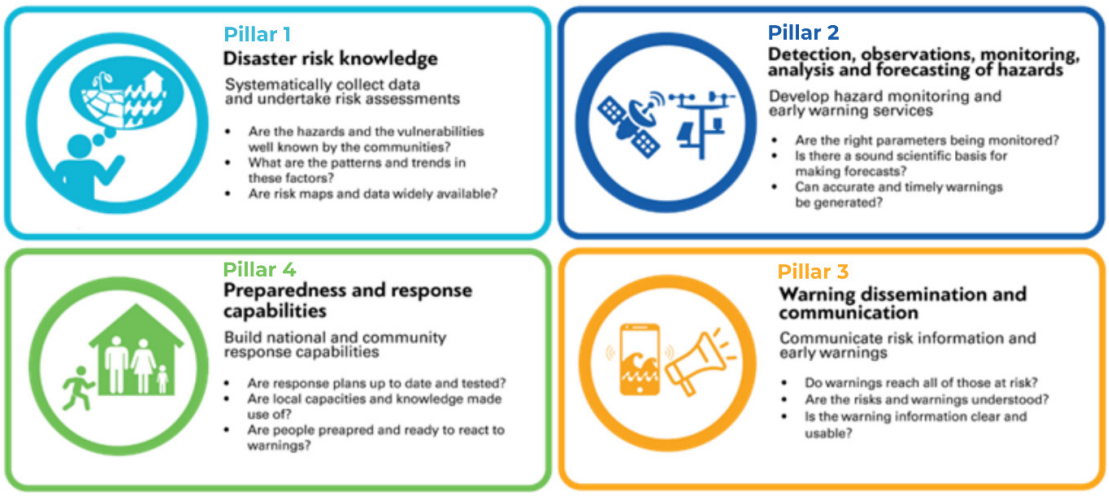
4 WMO. (2023). Early Warnings for All Initiative scaled up into action on the ground. Retrieved from: https://wmo.int/activities/early-warnings-all/wmo-and-early-warnings-all-initiative

5 WMO. (2022). Early Warnings for All: Executive Action Plan 2023-2027 (The UN Global Early Warning Initiative for the Implementation of Climate Adaptation). Available at: https://library.wmo.int/index.php?lvl=notice_display&id=22154

6 UNDRR. Early warnings for all. Retrieved from: https://www.undrr.org/early-warnings-for-all

- Define roles/responsibilities and, in general, strengthen the collaboration between key ministries, academia, the private sector and vulnerable communities to generate improved risk information.
- Ensure that all risk knowledge capability is locally led, where possible; people-centred and strengthened through an increased use of science.

Figure 2: Pillars of the EW4All Initiative.



Source: ITU.

For the second pillar (observation and forecasting for *early warnings*), the action plan centres in five key action areas:[7]

1. Enhancing capacity to detect hazards: The action plan proposes to conduct gap analyses on early warning needs, expand the cataloguing of hazardous events, an enhance the timely access to, and use of satellite observations and of advanced technologies to build up detection and forecasting capabilities.
2. Close the observing gaps to meet the data needs for monitoring hazards, including actions such as establishing and implementing the Global Basic Observing Network to deliver timely data to global weather prediction systems, and accelerating the implementation of the WMO action plan for hydrology, including establishing regional hydrological status systems (HydroSOS).
3. Enhance the existing framework and the capabilities of global data processing, forecasting, and analysis systems: this includes the expansion of the network of Regional Specialized Hydro-Meteorological Centres and the associated National Hydro-Meteorological Centres to meet region specific needs.
4. Sustainable data and Information exchange infrastructure to support EWS: Considers actions such as accelerating the implementation of the WMO Information System 2.0 (WIS 2.0) to enable timely and sustained data access and develop technical capabilities.
5. Optimize international efforts on observation, monitoring, and forecasting in support of EWS, as fostered by, for example, UNDP, UNEP and UNESCO, and upscale successful regional initiatives on sharing data and forecasting products.

Pillar 3 of the EW4All initiative (Warning Dissemination and Communication) is led by ITU with support from IFRC, Risk-informed Early Action Partnership (REAP), UNDP, and WMO. It focuses on ensuring that an identified risk and alert can reach those people at risk, including

[7] WMO. (2022). Early Warnings for All: Executive Action Plan 2023-2027 (The UN Global Early Warning Initiative for the Implementation of Climate Adaptation).

that the alert message is communicated and formulated in a way that those who receive it can understand and act on the alert, using a standardized and consistent format such as common alerting protocol (CAP).

In this third pillar, ITU highlights the use of multichannel dissemination alerting (including mobile networks, radio, TV, sirens, Internet, social media, satellite, etc.) and the opportunities that the spread of ICTs provide in reaching more people (i.e. increased mobile broadband networks and ownership of mobile devices). One key advantage of disseminating alerts through mobile networks is that these networks are geo-located, so warnings can reach only those users located in a specific risk zone. Also, this communication technology (called cell broadcast and often complimented with location-based SMS) allows for warnings adapted to specific user requirements, such as a certain language, among other possibilities (See cell broadcast (CB) and location-based SMS (LB-SMS)).

ITU has also highlighted that the pillar will focus on promoting a regulatory approach, based on the model adopted by several countries including the EU, which has mandated the use of geo-located alerts using mobile networks, and engaging the mobile network operators to implement mobile EWS systems.

According to the EW4All Executive Action Plan, expected outcomes for the third pillar include:[8]

- Define functions, roles, and responsibilities for each actor in the warning dissemination process through government policy.
- Ensure that warnings reach those at risk by using multichannel dissemination and communication alerting.
- Strengthened and expanded alert dissemination and feedback channels reaching all people with actionable information.
- Ensure the capability for effective, authoritative emergency alerting that leverages the common alerting protocol (CAP), suitable for all media and all hazards.

The fourth pillar relates to preparedness to respond, and focuses on the different actions to be taken in order to ensure that early warnings reduce loss and harm. That is, enabling and preparing people at risk to respond to warnings, to strengthening national and local stakeholder capacities. According to the action plan, the main outcomes in this pillar include:

- Crisis/disaster risk management and climate adaptation laws, policies and/or plans are reviewed, ensuring they reduce climate change impacts and exposure on people and the environment.
- Preparedness at the local level enables local first responders to act quickly and effectively based on the early warning alert.
- National and local actors monitor the availability of early warnings, associated financing, and the feasibility and effectiveness of anticipatory action.
- Strengthened collaboration between stakeholders generates informed actions on the ground.

[8] ITU. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Early-Warnings-for-All-Initiative.aspx

3.1 Cell broadcast (CB) and location-based SMS (LB- SMS)

In 2025, more than four out of five people around the world owned a mobile phone, with global active mobile subscriptions reaching 112 per cent, and network coverage available for 96 per cent of the world, at least with a 3G network[9]. This makes mobile networks an incredibly powerful communication channel to alert populations about an imminent hazard. Among mobile-based warning technologies, Cell Broadcast (CB) is widely regarded as particularly suitable for rapid, large-scale public alerting, as it can reach all compatible devices in a targeted area without relying on individual phone numbers and with limited impact on network congestion. Location-based SMS (LB-SMS) can complement CB by supporting more targeted follow-up communication, delivery reporting and two-way interaction in contexts where these functions are needed.

CB and LB-SMS rely on different technical approaches. CB is a point-to-area broadcast technology that sends alerts to all compatible devices connected to selected network cells within a defined geographic area. It does not require a database of individual phone numbers and can therefore disseminate messages rapidly to large numbers of people, including visitors and people temporarily present in the affected area. Location-based SMS uses subscriber mobile numbers for point-to-point communication, to send a message to all mobile phones detected in a risk zone.

In that sense, both cell broadcast (CB) and location-based SMS can support geo-targeted warning dissemination, while serving different functions. Additionally, the alerts can be adapted to specific requirements, such as a user's language, depending on the system configuration and available data.[10]

Cell broadcast (CB)

CB is a broadcast technology operating at the default granularity of a single cell up to any number of cells in a particular region.[11] It is a point-to-multipoint service that allows to send a text message to a specific area (local, regional, or nationwide), to a large number of subscribers, including visitors from other countries, and influx of users to the affected area. As there is no need to know the number of the mobile device to which a message will be sent, there are no privacy concerns with CB. This type of broadcast can also be repeated during a configurable period, or the message could expire after a single broadcast. When a CB message is received by the user, it is displayed automatically on the mobile phone screen accompanied by a special ringtone and/or vibration. The phone is blocked until the user acknowledges the alert. CB also allows text-to-speech in certain cases, and in the users´ desired language.[12]

---

9 ITU. Facts and Figures report. Available at: www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-mobile-network-coverage/.

10 Reliefweb. (2023). Mobile-based Early Warning Systems For effective and inclusive alerting Report; ITU. (2023). Early Warning Systems: Saving lives through mobile connection. Retrieved from: https://www.itu.int/hub/2023/01/early-warning-systems-mobile-connectivity/; and Everbridge. (2023). Location-based SMS: The smarter way to save lives. Retrieved from: https://www.everbridge.com/blog/location-based-sms/

11 BEREC. (2020). BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means.

12 European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.

CB has several advantages for rapid, large-scale public alerting, while also presenting some limitations compared to other options. Some of the main advantages of CB are:

- Message display: Messages can be broadcast in any language and displayed depending on the mobile device language settings[13]. In addition, the message is displayed without the need of user interaction, and it has a distinct warning tone and vibration pattern.[14]
- Message delivery: As CB works on a one-to-many basis, one message can be sent to millions of devices almost immediately.[15] Also, because a CB message is sent only once to each cell, and from each cell it is broadcast repeatedly to all attached mobile devices, the network load for a given warning message is very low. In addition, CB traffic is either carried with the highest priority (3G/4G) or on a dedicated channel (2G).[16] This means that this technology will always work, even when the network is congested.[17]
- Geo-fencing: Since 2019, CB has been enhanced to allow for geo-targeting, that is, using the mobile device geolocation capability to improve accuracy to levels equal to those of satellite navigation.[18] Using the network target area geometries (polygons and or circles), the geo-fencing feature can use satellite navigation and the cell information to establish location with an accuracy level of a few metres. Geo-fencing can help alert-originators to issue warning messages to specific areas, for instance, those living on the left side of the highway but not on the right.[19]
- Security: In CB, the recipients remain anonymous as this technology does not require registration of numbers or maintenance of a number database.[20]

However, compared to point-to-point technologies such as LB-SMS, CB has two main limitations: first, CB does not have the capability to provide confirmation of delivery in real time[21]; and second, it does not provide "follow-up" capabilities (less granularity), and it can only be used for one-way communications.[22] Some earlier limitations related to handset compatibility and user configuration have been reduced over time, as CB functionality is now supported by many modern devices and does not require users to subscribe to a service. However, compatibility and default activation should not be assumed in all contexts. Older handsets, operating system versions, market-specific device configurations and operator settings may affect whether CB alerts are received and displayed correctly. Countries implementing CB should therefore assess handset compatibility and default settings as part of implementation, in coordination with mobile network operators and device manufacturers.

Location-based SMS (LB-SMS)

Location-based SMS combines traditional SMS with cell-based location. It uses existing SMS channels combined with the accuracy of cell-based location to send the messages.[23] This allows governments, public agencies and mobile operators to send SMS notifications and warnings

---

13 European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.
14 GSMA. (2013). Mobile Network Public Warning Systems and the Rise of Cell-Broadcast.
15 Ibid.
16 BEREC. (2020). BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means.
17 European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.
18 Ibid.
19 One2Many. Why cell broadcast is more Important than ever for Emergency alerting!
20 GSMA. Cell Broadcast for Early Warning Systems.: A review of Technology and how to implement it
21 European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.
22 Everbridge. (2023). Location-based SMS: The smarter way to save lives. Retrieved from: https://www.everbridge.com/blog/location-based-sms/
23 European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.

to a list of mobile subscribers located in a specific geographical area.[24] In general, an LB-SMS message is an SMS message that is sent to a subset of mobile network attached devices in a particular geographical area.[25]

Given these characteristics, LB-SMS offers useful complementary functions in certain situations or for specific threats. Some of the advantages of LB-SMS technology are:

- Confirmation of delivery (bi directionality): Unlike cell broadcast technology, LB SMS provides confirmation of delivery and "service performance" data in real-time, as it is a two-way communication tool. This allows operators and authorities to store messages, showing a count of recipients, individual delivery reports, language specific content (based on recipients' country code), send updates, and receive feedback or replies by the users, which may provide vital information to emergency services, facilitate the monitoring of situations, and better plan the deployment of resources.[26] It may also be useful for demographic groups such as people with special needs, elderly, children, etc. to request assistance during evacuations.[27]
- Provides follow-up messaging (granularity): Allows customized messaging for vulnerable groups, and to send individual messages to certain numbers even if people have left the affected area. This can be particularly useful in certain situations, such as pandemics, where, for instance, a follow-up medical treatment is needed, or for hazards such as chemical attacks. [28]
- Service barring and familiarity: Users cannot by default opt out of LB-SMS, as their only way to do it is by turning off their device, setting it to silent or ignoring the alert.[29] Also, unlike other technologies, SMS are a universally known communication channel, which may facilitate alerting specific demographic groups such as people with special needs or the elderly. Traditional messaging may also provide lesser chances of causing panic while sending alerts for incidents that can be predicted a few days in advance.[30] This characteristic, nonetheless, may be seen as a disadvantage, as traditional messages can be easier to disregard: these messages look similar to any other messages sent to a phone.

Although these advantages allow an efficient use of this technology in certain situations, LB SMS also presents some disadvantages and limitations:

- The use of classical SMS requires having a number database: This technology is ideal as a personal one-to-one messaging solution but requires the establishment and maintenance of a database of target numbers for bulk messaging[31]. In other words, for all areas where mobile network operators (MNOs) deliver messages, a list of all users currently located in those areas must be kept up to date. This is usually not the case at the granularity of the single cell level, as knowledge of subscriber location is not required for normal operation. in addition, this may limit dissemination of information for persons at risk who are not subscribers of specific MNO services (e.g. tourists). [32]

---

[24] Opecode. Opencode location-based SMS Broadcast. Retrieved from: https://opencode.com/emergency-advanced-mobile-location-aml-gateway

[25] BEREC. (2020). BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means.

[26] Everbridge. (2023). Location-based SMS: The smarter way to save lives. Retrieved from: https://www.everbridge.com/blog/location-based-sms/

[27] European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0

[28] Everbridge. (2023). Location-based SMS: The smarter way to save lives. Retrieved from: https://www.everbridge.com/blog/location-based-sms/

[29] European Emergency Number Association (EENA). (2019). Public Warning Systems – version 3.0.

[30] Ibid.

[31] GSMA. (2013). Mobile Network Public Warning Systems and the Rise of Cell-Broadcast.

[32] BEREC. (2020). BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means.

- Network congestion: Even though the capacity of networks has been increased in recent years[33], this technology requires the use of networks that are often severely congested during emergency situations, causing delays in message delivery.[34]
- Security: Unlike other technologies, where messages can only be sent by authorized personnel who have been given access to the system, in LB-SMS, messages can be sent from any source, however, the identity of the sender is difficult to verify.[35]
- User interface: This technology cannot over-ride the mute function and it does not necessarily make the phone vibrate.[36]

Table 2: Summary of CB / LB-SMS characteristics

Characteristic	LB-SMS	CB
Transmission type	Point-to-point	Point-to-area
Mobile number dependency	Requires database of phone numbers	Does not require database of phone numbers
Bi directionality	Yes. Users can respond directly to sender	No. Message should contain a URL or number to reply
Granularity	Allows follow-up messaging and customized messages for specific numbers	No follow-up or customized messaging
Congestion	Subject to network congestion	Always available
Security	Source of message cannot be verified	Only mobile operator or authorities can broadcast messages
Service barring	No barring	Users can turn off CB reception
Delivery Confirmation	Yes	Not available
Repetition rate	No	Message can be repeated between 2 sec. and 32 min.
Language Selection	Only based on recipients' country code	Yes

Source: ITU, based on One2Many. (2012)[37]

In general, CB and LB-SMS can both be very useful when disseminating early warnings or information during the disaster response phase. Cell broadcast instantly sends loud distinctive alerts to a very wide coverage without congesting the network, while location-based SMS makes it possible to send alert messages point-to-point in a specific area. These technologies are

[33] Ibid.
[34] GSMA.Cell Broadcast for Early Warning Systems.: A review of Technology and how to implement it.
[35] Ibid.
[36] Everbridge. (2023). Location-based SMS: The smarter way to save lives. Retrieved from: https://www.everbridge.com/blog/location-based-sms/
[37] One2Many. (2012). White Paper – Cell Broadcast Emergency Alerts.

complementary[38], and it is highly recommended to deploy both. DRM authorities can use CB for larger-scale emergencies, for instance, that require a large number of people to be alerted, or for events that are more likely to congest the mobile network, such as earthquakes, tsunamis, or hurricanes. LB-SMS can be used for prolonged emergencies that require regular updates, such as heat waves or pandemics. Table 2 compares the main characteristics and capabilities of both LB-SMS and CB technologies.

[38] The EU legislation, nonetheless, only requires implementing at least one of the two technologies. See: https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-how-to-assess-the-effectiveness-of-public-warning-systems-transmitted-by-different-means-0

4 Legislation related to disaster risk management

Legislation and regulations are key for DRM, as they define the roles and responsibilities of stakeholders involved in the DRM process. These legal frameworks determine the coordination mechanisms, communication channels and standard operating procedures, and identify decision-makers in relevant agencies who have a role in DRM.[39]

It is important to confirm and assess a country's current legislative and regulatory DRM framework as part of the development of NETPs is based on this framework.

Constitution

The legal framework of the country for which the NETP is being developed should identify the authority which declares and manages emergencies as well as the telecommunication/ICT services that are supplied.

Emergency powers

The scope of emergency powers and how they are declared and used in the context of a national emergency should also be defined.

National disaster management

The legislative framework that establishes the entities, organizations and processes must be defined and declared. It is expected that relevant legislation will either be in place or will be required as part of the NETP that will address:

- disaster management
- national security
- works
- housing
- telecommunications
- health and the environment
- social development and mobilisation
- energy

It is also expected that national disaster management policies and plans will be identified that will address various essential factors addressing provisions for the prevention, preparedness, response, and recovery in relation to disasters, including:

- Procedures relating to disaster management of ministries and departments of government, statutory bodies and other agencies, organizations or persons who perform functions under the relevant legislation,
- Procedures for coordinating the implementation of the national disaster management plan with the above.
- Procedures for informing the persons identified above, the general public in the country in question and elsewhere of the existence of a disaster or disaster alert.

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

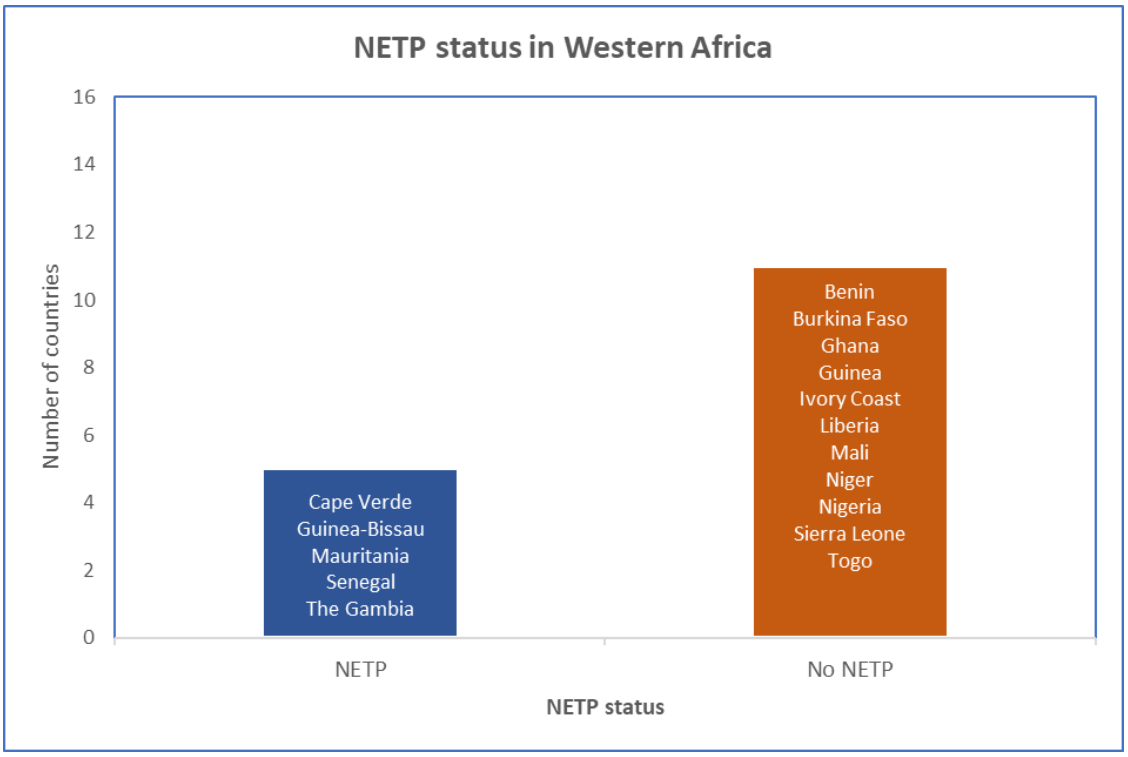
- Procedures for preparing and maintaining inventories of services, systems and supplies for disaster management.
- Procedures for mobilisation of the above during a disaster alert or disaster, including procedures for staffing relevant organizations and operational centres for disaster management co-ordination.
- Procedures for protecting and restoring communications, both nationally and internationally during a disaster or disaster alert.
- Procedures for procuring, releasing, distributing, and replenishing contingency stores of supplies during a disaster or disaster alert.
- Procedures for providing shelter for persons during a disaster or disaster alert.
- Procedures for cooperating with international organizations and governments of countries outside of the country during a disaster alert or disaster.
- Procedures to apply if the evacuation of residents of an area is considered necessary if there is a disaster.

Declaration of disaster: Legislation should set out how and when the relevant office holder within the country declares, after consultation with the relevant colleagues that there is a substantial prospect of any of the following: earthquake, fire, flood, hurricanes, landslides, major earth movement, storm surge, tsunamis, tidal waves, volcanic eruptions or other hazard, within the timescales indicated within the legislation. The scope of the disaster, whether it is nation-wide or restricted to a specific area or region, should also be established. In so doing, the relevant responsible person determines that the relevant government departments, or other person(s) so authorised under the legislation, should exercise the powers granted under the legal provisions to prevent or minimise the loss of human life, illness or injury to humans, property loss or damage or damage to the environment. Once it has been determined that the disaster and the need for disaster response has passed, the relevant responsible person, (normally the Head of State or other identified person) shall declare the end of the disaster and that it is no longer necessary for persons exercising disaster powers to do so.

Action Item 1: Development of legislation for DRM

Legislation for disaster risk management should be documented in the NETP and if it does not exist then it should be created made official, easily accessible and maintained. Ideally this should be on-line and maintained such that when any of the different elements are added to or updated, the changes and additions are reflected in the other elements. For example, relevant legislation should consider referring to the Tampere Convention, if the country has acceded to it and if not, serious consideration should be given to incorporating its provisions and ensuring they are implemented and communicated to all stakeholders so they can embrace them in their DRM plans.

Figure 3: NETP status in Western Africa



5 National disaster management policy

Where appropriate, the legislative structure should establish a national disaster management policy for the country. This should be based on the requirements of national emergency and disaster management legislation and sets out a vision for emphasising preparedness on the part of government, sectors, communities, stakeholders, and individuals in targeted DRM activities.

Key performance indicators should be defined for each of the policy objectives identified, to help drive implementation. A set of conditions should also be identified that will be used to guide and direct the achievement of each objective, to assure the solutions implemented are in keeping with the general themes of the policy framework. These conditions could include:

- Disaster response interventions should be based on early warning systems facts and credible information which is disseminated in a timely manner.
- The right to receive relief should be enjoyed by all citizens regardless of race, political affiliation, gender, religion, or geographical considerations.
- The provision of assistance should be based on a thorough post disaster needs assessment of the affected populations or their available local capacities to meet those needs.
- Culture and customs of those affected should be respected during the provision of assistance.
- Disaster assistance should strive to maintain health and wellness and reduce future vulnerabilities as well as meet basic needs.
- Communities should be involved in the design, planning, implementation, monitoring, and evaluation of interventions meant to benefit them.
- Stakeholders should recognise the need for gender equality and ensure equity in participation and in sharing benefits across all segments of affected populations.
- Negative impacts to the environment should be avoided or minimised to foster sustainability of the physical and natural environment.

International humanitarian assistance: The policy should define how the country interacts with international humanitarian assistance agencies before, during and after a disaster.

Other provisions: The policy may set out the basis for establishing a government agency responsible for disaster risk management and establish to make regulations regarding early warning systems; volunteers, hazard inspectors and evacuation; types of hazards and disasters; the collection and publication of data pertaining to disaster risk management; and for the provision of recovery assistance.

Action Item 2: Maintenance of a national disaster management plan

A national disaster management plan should be created, if one does not already exist, this should be updated and published, and the most recent version should be made accessible, based on the legislation for disaster risk management currently in force. The authorities in charge of disaster risk management in the country should incorporate the Tampere Convention's provisions in the disaster management plan if necessary, making the necessary regulatory adjustments, complementing the current regulations on international assistance for disaster risk management. These, and any necessary further steps, will help all those involved in disaster risk management to internalize and effectively adopt this legal framework for cooperation and embed it the operations and practises of all relevant stakeholders.

It should include up-to-date information regarding coordination between relevant actors involved in DRM, as well as the emergency response communications network and the necessary telecommunications equipment and services, among other elements, identified by the NETP and show greater alignment with any prevailing comprehensive disaster management plan or policy within the nation-State concerned.

6 Agencies Involved in disaster risk management

The relevant actors in relation to emergency telecommunication management should be described along with their inter-relationships. This should include identifying those agencies that are responsible for regulating, delivering or intensively dependent on telecommunications/ ICTs.

Action Item 3: Integration of plans and policies

Ensure the responsible agencies, government departments and other entities involved with comprehensive disaster risk management and associated telecommunications/ICTs within the country are appropriately identified including any inter-relationships, shared or devolved responsibilities.

Table 3: Disaster management authorities involved in the NETP

Authorities	Typical role in the NETP
National disaster management authority	Leads or coordinates disaster preparedness, response, and recovery, and should serve as a core institutional partner in the NETP.
Ministry or agency responsible for telecommunications/ICTs	Lead entity for the development of the NETP. Provides sector oversight, regulatory coordination, and engagement with telecommunication operators and ICT service providers.
National telecommunication regulator	Supports regulatory arrangements, spectrum issues, operator obligations, and emergency communications coordination.
Emergency operations coordination centre	Serves as the operational hub for inter-agency coordination and information-sharing during emergencies.
First responder agencies, such as Red Cross/Red Crescent, fire-fighters, civil defense	Identify operational communication needs and ensure interoperability for field response.
Meteorological / hydrological / geological and other hazard-monitoring agencies	Provide hazard detection, forecasting, and technical inputs that trigger monitoring and warning for emergency communications.
Health authorities	Ensure continuity of health emergency communications and coordination during public health emergencies and disasters.
Security and civil protection agencies	Support public safety communications, national security coordination, and response operations where relevant.
Local / subnational disaster management authorities	Adapt and implement NETP arrangements at provincial, district, municipal, or community levels for contingency plan development.
Telecommunications operators and service providers	Maintain, restore, and support continuity of telecommunicationnetworks and services during emergencies.
Critical infrastructure operators	Coordinate dependency management, especially where telecommunicationservices support power, transport, water, and emergency services.

7 National development plan

Ideally there should be a wider national development plan or equivalent in place that sets out a strategic direction for the future of the State along with policies and provisions to guide future development and define a clear framework for future investment. It should aim to guide public and private sector actors as well as non-governmental organizations (NGOs) and community-based organizations (CBOs).

A key part of the strategy should call for the building a multi-hazard resilient country; that is, for the country to reduce the impact of, and time to recover from, the impact of climatic and other natural shocks that can often occur simultaneously, as well as boosting the overall socioeconomic development trajectory of the country. One of the key parts of such a strategy should the development of the telecommunication Infrastructure.

Action Item 4: Integration of plans and policies

The development plan should set out a general policy calling for the support for proposals that facilitate communication during emergencies. There should be a link to the national disaster plan, reference to the comprehensive disaster management policy, and this national emergency telecommunication plan as proposals are developed and considered, to ensure they are up to date, consistent and aligned. A key goal should be to drive the extension and availability of telecommunication infrastructure to support development aims in general and specifically ensuring telecommunications/ICTs can be exploited to the maximal extent in the four phases of emergency preparedness and response. This must address how the telecommunication/ICT infrastructure can improve early warning detection of hazard alerts and the dissemination and communication of alerting information to all parts of the population, including any marginalized groups.

Mitigation phase

8 Vulnerability to disasters from natural and technological hazards

Due to the unique geographic, topographic, and hydrological characteristics of a specific country, it may be vulnerable to different types of hazards, particularly earthquakes, floods, hurricanes, landslides, storm surges, tsunamis, and volcanoes. In addition, there may be hazards derived from the technological infrastructure of a given country, including road, rail, air and maritime transportation links The Appendix to this document provides information on the type of hazards that countries phase.

8.1 Natural hazard maps

The production and maintenance of hazard maps is an essential part of the NETP since it guides the design and development of telecommunication/ICT systems, enables areas of risk to be identified and enables areas of need to be highlighted. This also aids the establishment and maintenance of early warning systems, the design and development of shelters and the planning for the deployment of resources in the event of a disaster. It is crucial that these maps are curated by a responsible authority within the country to ensure they are comprehensive, up to date and easily accessible by key stakeholders.

Volcanic: The volcanic hazard map(s) should identify all areas within the country and any adjacent areas that represent potential volcanic hazards. If there are none, this section could be deleted.

Coastal surges and flooding: The costal surge and flooding hazard maps should identify all areas within the country that are susceptible to coastal surges or flooding. If there are none, this section could be deleted.

Landslides: The landslide hazard maps should identify all areas within the country that are susceptible to Landslides. If there are none, this section could be deleted.

Earthquakes: The Earthquake Hazard Maps should identify all areas within the country that are susceptible to earthquakes. If there are none, this section could be deleted.

Action Item 5: Creating and Maintaining Hazard Maps

Maintaining and ensuring hazard maps for the different types of hazards exist is an essential contributor to disaster planning and the development of mitigation strategies. Information must be detailed at the municipal level and should be available to telecommunication/ICT operators to ensure they consider these factors in infrastructure planning and resilience. Also, it should include information on the most vulnerable communities, specifying the type of hazards they are prone to, as well as the communications resources available in each of them. This activity could be carried out with the support of the responsible authorities and relevant planning departments and go beyond the practise of collating GIS information to become proactive curation of this data, identifying gaps and driving project requirements to expand and maintain GIS/hazard map information.

8.2 Technological hazards

In contrast to the various sources of natural hazards that may impact a country, various man-made technologies can be the source of catastrophic disaster. A number of these are tracked and recorded in the EM-DAT data on emergency incidents and disasters[40] and highlighted in the following sections which should be edited to ensure the most appropriate ones are considered when this template is edited for a specific country.

Road transportation: Depending on the road network within a given country, incidents may have a very significant impact on a particular nation in terms of the effects on people, property, economy, or environment.

Rail transportation: Depending on the rail network within a given country, incidents may have a very significant impact on a particular nation in terms of the effects on people, property, economy, or environment.

Air transportation: Depending on the geography of a given country, air transportation incidents may have a very significant impact on a particular nation in terms of the effects on people, property, economy, or environment.

Marine transportation: Depending on the geography of a given country, air transportation incidents may have a very significant impact on a particular nation in terms of the effects on people, property, economy, or environment.

Cybersecurity: As nations become increasingly reliant on telecommunications/ICTs for commerce, e-government, international trade, education, healthcare and many other applications, the risks associated with cyber incident hazards become ever more significant. Appropriate assessment of a country's national cybersecurity posture is therefore increasingly important.

[40] Ibid.

9 Telecommunication/ICT sector

This section of the NETP must identify all aspects of the telecommunication/ICT sector within the country, including the identification of all the public service operators for fixed, wireless, mobile, broadband, Internet, broadcast television, broadcast radio, subscription television, satellite and any other relevant capability including amateur radio.

Action Item 6: Service provider supporting policies and procedures

The public network service operators should be asked to provide details of their business continuity and disaster management processes and procedures. This activity could be carried by the telecommunication regulator with support of any government department responsible for disaster management. This should also include any relevant planning departments to ensure alignment.

Mobile **services**: The service providers offering public mobile telecommunications services must be identified along with any relevant policies and procedures. This section should include the description of all public mobile service providers operating within the country, along with the network coverage maps. Relevant maps for GSM, 3G and 4G/LTE services can be accessed via the GSMA Coverage Maps platform and should be extracted and updated as appropriate.

Action Item 7: Early warning capabilities

Support for early warning capabilities should be established from the point of view of both hazard detection and dissemination of alerting information to as wide a range of communications channels as possible and the role that service providers can fulfil. It is essential that whatever combination of solutions are deployed, that they deliver timely, accurate and actionable information to all population groups. The use of standard based protocols, such as the common alerting protocol (CAP), should be assessed to maximize interoperability between service providers and between the government department responsible for disaster management and each service provider. This should also solicit information on the mechanisms supported that enable national coverage and localisation of alert messages, such as cell broadcast and location-based SMS and identify any constraints associated with these. This should also include consideration of any indication concerning 2G/3G closure and migration to 5G radio and any impact on early warning that may result from that, including the impact on monitoring devices/equipment and the gathering and dissemination of warning information.

Once these aspects have been confirmed, this NETP should be updated with the information obtained.

Fixed services: The service providers offering public fixed telecommunications services must be identified along with any relevant policies and procedures.

Emergency communications network (ECN): An emergency communications network (ECN) will be a network dedicated to the use of the emergency services and main stakeholders to carry critical communications during an emergency. It will typically be constructed using digital mobile radio (DMR) technology as specified in ETSI TS-102-361-1 or equivalent, Terrestrial Trunked Radio Access (TETRA) technology as specified in ETSI EN 300-392-1 or newer solutions such as those derived from ETSI TR-103 219-1 for 4G, 5G and in the future 6G mobile networks. It should be identified within the NETP and defined in terms of scope and reach of the services and

coverage it provides, along with connections with the various agencies it supports. Emergency communications networks typically provide a number of features including point-to- point voice, push-to-talk voice, GPS location services and supervisory control and data acquisition (SCADA). This type of deployment would be expected to operate under licensed conditions[41] to minimise interference from other networks, applications, and users.

Action Item 8: Emergency communications network

Where an ECN is implemented, coverage maps for the entire nation need to be established and any gaps identified that could limit coverage in an emergency scenario. Furthermore, spectrum licensing should ensure the ECN uses dedicated radio bands that are protected for this purpose. Consideration should also be given to the interconnection of this system with the fixed and mobile networks operating to ensure ease of use across all areas of the country. Furthermore, the ECN should be assessed in the context of command and control for Early Warnings for All Initiative alert communications.

Maritime communications: Where the NETP is being developed for a country with a significant marine environment, consideration should be given to communications supporting this environment. This should include VHF radio and Global Maritime Distress and Safety System (GMDSS) services amongst other formats and consider how they will be connected into fixed, mobile and emergency communications networks. Consideration should also be given to how the maritime communications environment can participate in a wider early warning capability.

International connectivity: International connectivity should be identified in the NETP, along with the operators of any such infrastructure.

Subscriber television network: The subscription television services (Pay TV) that are operating within the country should be identified, as they may provide a conduit for propagating warning messages, alerts and so forth.

Television broadcast network: Television broadcast networks operating within the country should be identified along with the significant role they can play in dissemination of early warning alert information.

Broadcasting: Broadcasting services operating within the country should be identified along with the role they play in disseminating authorised alerting information and updating all stakeholders, community groups and the population as a whole during disasters and training events.

Amateur radio: Amateur radio[42] can play a significant role in disaster response, if the appropriate communities are engaged, trained, and organized alongside more formal telecommunications/ ICTs. They can often play an important role in connecting marginalized communities and communicating disaster alerts and warning information.

---

41 System Reference document for harmonized use of Digital Mobile Radio (DMR) ETSI TR 102 335-2 V1.1.1

42 https://www.iaru-r1.org/about-us/committees-and-working-groups/emcomm/emergency-operating-procedures/

Action Item 9: Network inventory and coverage

Update the network inventory and coverage of mobile and fixed telecommunication*/ICT operators, and radio and television broadcasting. Also, maintain an updated database with the focal points in charge of technical aspects as well as with those in charge of communication of alerts and relevant information regarding disasters as part of the dissemination and communication aspects of achieving early warnings for all. Include network information and coverage of radio amateurs and first responders (police, firefighters, etc.) and identify any gaps. Assess the implementation of other options on* telecommunication*/ICT infrastructure, such as satellite services, including satellite devices for voice/broadband communications and consider the possibility of community WiFi to strengthen emergency response and recovery activities.*

10 Vulnerability analysis of critical telecommunication/ ICT infrastructure

The different telecommunication operators and the government agencies responsible for government telecommunication/ICT networks must develop and present a vulnerability analysis of the critical infrastructure of their networks, based on the risk maps and assessments of the different types of hazards.

Telecommunication operators should include coverage maps of their networks in this vulnerability assessment, as well as an inventory of the telecommunication infrastructure, and evaluations regarding power supply to support it, and capacity to manage maintenance of the telecommunication infrastructure and equipment.

As governments become increasingly dependent on digital infrastructure, it is important for cyber security considerations to be considered by the government institutions, businesses, and citizens.

Susceptibility to outbreaks of disease which may impact the community at large and therefore the availability of people to resource the operational management of the telecommunication/ ICT infrastructure during periods of seasonal, epidemic, or pandemic illness also need to be considered.

Action Item 10: Vulnerability analysis

All telecommunication/ICT service operators, mobile, fixed, and radio and television broadcasting operators, as well as government networks, in conjunction with the relevant regulatory body, should develop (or update) and present for approval to the government agency responsible for disaster management a vulnerability analysis of the critical infrastructure of their networks, including an inventory of the infrastructure, and power, maintenance and connectivity evaluations along with consideration of the risks associated with cyber security or other technological factors. This should also consider how the telecommunication/ICT services will participate in a national Early Warnings for All Initiative solution.

11 Specific telecommunication/ICT regulatory framework for disaster management

This section of the NETP should identify all the key pieces of regulations and policies that define the framework for telecommunications/ICTs within the country, and particularly those elements that impact disaster management.

11.1 Mitigation phase and preparedness phase

1. The telecommunication service providers could be obliged to carry out the vulnerability analysis of the networks according to the risk maps in different geographical areas and to establish the corresponding contingency plans that guarantee, to the extent possible, vital communications for emergency management, as well as for the timely restoration of user communications. These plans should be submitted to, and approved by, the regulator.
2. Commercial and community radio broadcasting operators, as well as public and private television broadcasting operators should transmit information campaigns for the prevention of disasters and emergencies. These campaigns must be developed in coordination with the government agency responsible for disaster risk management and the telecommunication/ICT regulatory authority and should have a prescribed duration and broadcasting chronogram.
3. Regulations for temporary spectrum licences for up to 6 months, extendable only once, should be implemented to allow telecommunication/ICT providers to offer services during the response and recovery phases of disaster risk management.
4. Temporary spectrum licences, as well as special service licences, granted specifically for the purpose of facilitating communications during emergency response and recovery, should be exempted from any type of charge.
5. Regulations to implement the Tampere Convention should be established or otherwise made more obvious as to the provisions acceded to.
6. The government should decide on a specific model to utilize the spectrum allocated for public safety, including considering the potential options for:

    - Dedicated network: spectrum to be used exclusively by public safety.
    - Shared network: support both public safety and commercial usage with different network cores and priority access and pre-emption rights for public safety.
    - Commercial network: public safety uses the mobile commercial networks.

11.2 Response phase

1. To avoid network congestion, mobile service providers should encourage the use of SMS texting by its customers. Also, they could limit the duration of calls; for example, by establishing a maximum call duration of two minutes in the geographic area of the disaster during a period of 12 hours following the event that generates the emergency. These norms would not apply to calls made from or to the numbers of the authorities involved in the emergency response and should be aligned with the proposed regulation on the matter established in the regulatory framework.
2. Commercial and community radio broadcasting operators, as well as public and private television broadcasting operators could be obliged to transmit the messages that the National Emergency Management Organization (NEMO) determines to inform and update the public about the disaster. These messages could also include helpful contents regarding health services, shelter, food, and family reunification, among others.

3. Telecommunication service providers could be obliged to immediately assess the damage to their networks and implement their contingency plans to re-establish communications as soon as possible. There should also be a provision to report on the state of the network to the National Telecommunications Regulatory Commission – NTRC periodically.

11.3 Recovery phase

Commercial and community radio broadcasting operators, as well as public and private television broadcasting operators could be obliged to transmit the messages that the government agency responsible for disaster management determines to inform and update the public about the disaster. These messages could also include helpful content regarding health services, shelter, food, and family reunification, among others.

Action Item 11: Alignment and development of regional regulations

The government should develop specific regulations for the telecommunication/ICT sector regarding disaster risk management in the country. This includes establishing specific regulations based on the functions granted by the legislation, for each of the phases of disaster risk management, encouraging telecommunications operators to actively participate in each phase of disaster management.

Table 4: Countries with regulations for ICTs for disaster management

Country	Regulation
Benin	Benin utilizes a comprehensive legal framework for disaster risk management (DRM) that incorporates ICTs, including the 2023–2026 National Digital Security Strategy and the 2023–2027 National Artificial Intelligence and Big Data Strategy. These frameworks support early warning systems (EWS), telecommunication-based alerts, and digital tools for emergency management.
Burkina Faso	Burkina Faso primarily utilizes Law n° 012-2014/AN (2014) to govern disaster risk management (DRM), which creates the legal framework for using ICTs in early warning, risk monitoring, and emergency response. The law mandates information dissemination to the population and supports digital infrastructure for disaster preparedness, particularly through initiatives such as the Emergency Telecommunications Cluster (ETC) support in Burkina Faso.
Cape Verde	Cape Verde has established legal frameworks for ICT use in disaster management, primarily through the Civil Protection Base Law (Law no. 12/VIII/2012) and the National Disaster Risk Reduction Strategy (Resolution 114/2018), which promotes using information technologies to integrate risk reduction into national planning.
Gambia	Supported by the National Disaster Management Act 2008 and the new National Disaster Risk Management Policy 2023-2033, which emphasize integrating modern ICT tools for disaster resilience.
Ghana	Ghana utilizes legislative frameworks, primarily through the National Disaster Management Organization (NADMO) established by Act 517 (1996), to manage disasters. Regulations permit the use of mobile networks for alerts, though implementation focuses on coordinating traditional media such as radio alongside newer digital tools.

Table 4: Countries with regulations for ICTs for disaster management (continued)

Country	Regulation
Guinea	Guinea has a foundational law for disaster management, primarily established under Law L-96-009 of July 22, 1996, which covers risk management and creates structures such as the National Disaster Management Committee. While this legal framework outlines responsibilities, it is currently undergoing updates to better address modern challenges and strengthen the integration of ICTs.
Guinea Bissau	Guinea-Bissau is actively developing regulations and frameworks for ICTs in disaster management, primarily supported by ITU to strengthen emergency telecommunication preparedness.
Ivory Coast	Ivory Coast has established legal and strategic frameworks incorporating ICTs for disaster management, primarily through its National Strategy for Risk Reduction and Disaster Management (2020-2030) and the 2021–2025 National Cybersecurity Strategy.
Liberia	Liberia has integrated ICT regulations for disaster management through its National ICT Policy 2019-2024 and a national disaster risk management policy, focusing on early warning systems, emergency telecommunications, and business continuity.
Mali	Mali has a disaster risk management framework in place, aligned with international standards, that utilizes ICTs for early warning systems and disaster preparedness. While specific, localized legislation for ICTs in disaster management is evolving, national policies support the use of technology to build resilience against floods and other hazards.
Mauritania	Mauritania is actively developing legal and technical frameworks for ICTs in disaster management, transitioning from policy to operational implementation.
Niger	Niger has been mapping its legal framework for disaster risk management and international disaster response, but specific, comprehensive legislation focusing on the integration of ICTs for disaster management is in the development phase, rather than a firmly established, widely documented national law.
Nigeria	Nigeria has regulations and frameworks for using ICTs in disaster management, primarily guided by the National Emergency Management Agency (NEMA) and the Nigerian Communications Commission (NCC).
Senegal	Senegal is developing legal frameworks and strategies to incorporate ICTs into disaster risk management, focusing on early warning systems, cybersecurity, and digital governance. While specific legal acts for ICT-disaster use are evolving, key strategies include the SNC2022 Senegalese National Cybersecurity Strategy and a proposed national strategy on disaster risk finance.
Sierra Leone	Sierra Leone has regulations and policies incorporating ICTs for disaster management, primarily guided by the National Disaster Management Agency (NDMA) Act of 2020 and the National Digital Development Policy 2021.
Togo	Togo integrates ICTs for disaster management through policies and frameworks, such as the National Civil Protection Agency (ANPC) established by Decree 2017/11. Efforts are ongoing to strengthen early warning systems via ICT tools for flood monitoring and disaster risk reduction.

12 International conventions and treaties

The main international conventions and treaties to which the country developing the NETP belongs with respect to disaster risk management and telecommunications should be presented below. The NETP should highlight those aspects of the relevant international treaties the country is signatory to that impact disaster management, recovery, and planning. There should be appropriate consideration of transport links supporting the movement of material and equipment for natural hazard prevention and mitigation.

Among other mechanisms of cooperation, agreements should be sought that promote the following:

1. The gradual and progressive formulation and implementation of standards and laws, policies and programmes for the management and prevention of disasters caused by natural hazards.
2. Joint actions, with a view to identifying, planning, and undertaking programmes for the management of natural hazards with the assistance of specialized organizations operating in the region.
3. Cooperation in the formulation, funding, and implementation of aid programmes for those parties that request them, especially regarding assistance from regional and international organizations.
4. Periodic exchange of information, by diverse means, concerning best practices and experiences in the reduction of disasters.
5. The adoption of existing standards for the classification and management of humanitarian supplies and donations with the purpose of improved transparency and efficiency in humanitarian assistance.

Also, regarding scientific and technical cooperation, agreements should be sought that promote activities geared towards the following:

1. The creation of a roster of experts to facilitate impact evaluation missions in collaboration with the sub-regional, regional, and international agencies or teams that have already been established.
2. Conducting inventory in the field of prevention and mitigation and other related aspects of disaster risk management.
3. The identification of opportunities to strengthen intra and inter-regional co-operation, including academic institutions and research centres.
4. The exchange of technical materials and reports concerning the management of natural hazards.
5. The preparation, circulation, and continual updating of a register of qualified people in different disciplines to assist the region in the event of disasters.
6. Unification of the methodologies, lexicon, and other aspects of the terminology of natural hazards, for use by the signatory countries.

Agreements should be sought to establish common guidelines and criteria regarding different methods of disaster risk management, such as the promotion of the continuous training of personnel in areas that include health, emergency response and telecommunications, or the development and improvement of early warning systems at the regional, sub-regional and national levels.

Action Item 12: International cooperation

The relevant government departments must establish specific regulations for the implementation of the Tampere Convention where that has not already been achieved.

Coordination and collaboration with different international agencies such as the ETC (Emergency Telecommunications Cluster) and ITU (International Telecommunication Union) on issues of prevention and response to eventual disasters or emergencies is imperative.

12.1 Tampere Convention

This treaty helps relax barriers that impede the flow of information between the various elements of the international network for disaster response. Including, among other elements, establishing immunity against the confiscation of equipment, the prompt issuance of the corresponding licenses (e.g. telecommunication licences, use of spectrum, etc.), the development of mechanisms for the timely export of the equipment that was used under the Convention, and facilitating approval of the departure of the assistance personnel to their country of origin.

It is important that the authorities in charge of disaster risk management in the country incorporate the Tampere Convention provisions in the final version of the currently developing disaster management legislation, and make the necessary regulatory adjustments, complementing the current regulations on international assistance for disaster risk management. These steps will help all those involved in disaster risk management to internalize and effectively adopt this legal framework for cooperation.

In accordance with the above, and within the framework of the Tampere Convention, the responsible authority regarding telecommunication/ICT regulation must establish specific regulations for the implementation of the Convention, including, for example:

1. Exempt from any type of charge, including charges for the use of radio spectrum and for service license, among others, international aid provided through the Tampere Convention.
2. Temporarily and expeditiously issue any authorization for the use of the radio spectrum that is necessary, in line with the provisions of national legislation.
3. Simplify or exempt any other existing regulation that prevents the use of telecommunication/ICT resources from international aid under the Tampere Convention.

it is also recommended to inform the government entities of the cooperation framework so that stakeholders have a clear knowledge of the relevant legal provisions and can effectively apply them when a disaster strikes.

Table 5: Tampere Convention signed/ratified

Country	Tampere Convention
Benin	18 Jun 1998 Signature
Burkina Faso	No
Cape Verde	22 Mar 2018 Accession
Gambia	No

Table 5: Tampere Convention signed/ratified (continued)

Country	Tampere Convention
Ghana	18 Jun 1998 Signature
Guinea	8 Oct 2002 Accession
Guinea-Bissau	8 Oct 2002 Accession
Ivory Coast	No
Liberia	16 Sep 2005 Accession
Mali	18 Jun 1998 Signature
Mauritania	18 Jun 1998 Signature
Niger	18 Jun 1998 Signature
Nigeria	No
Senegal	20 Nov 1998 Signature
Sierra Leone	No
Togo	No

12.2 International cooperation

Finally, there are other mechanisms within the various frameworks of international cooperation that may be available to improve disaster risk management, provide adequate, sustainable and timely provision of support, including through finance, technology transfer and capacity building from international cooperation, tailored to their needs and priorities, as identified by them. In that sense, the United Nations Office for the Coordination of Humanitarian Affairs, for example, the United Nations International Strategy for Disaster Reduction; or the Emergency Telecommunications Cluster (ETC), can offer a set of tools that countries can use to promote more efficient disaster risk management.

In relation to international cooperation for the management of telecommunication/ICTs for disaster risk management, it is recommended that countries work together with ITU, considering it develops different activities on issues of telecommunications for emergencies. These activities include the publication of manuals on emergency telecommunication; emergency radio-communications specifications applicable to all phases of a disaster; databases of available frequencies for emergency radio-communication services on land and space, and the International Emergency Preferences Scheme and a common alert protocol-based infrastructure for communicating emergency alerting information, among others.

Preparedness phase

13 Standard operating procedures (SOP)

Standard operating procedures (SOPs) are defined as formal written guidelines or instructions for incident response. They generally have both operational and technical components and allow emergency response personnel to act in a coordinated manner across all disciplines in the event of an emergency.[43] These detailed instructions or procedures promote a uniform and standardized response during emergency response operations. These SOPs should be aligned with the legislative and regulatory frameworks as well as with the specific policies and plans related to DRM.

In addition, from a technical point of view, SOPs should consider the existing interoperability possibilities and, if necessary, the allocation of radioelectric spectrum in a specific band that allows communication to take place, based on the existing radio equipment. As such, it is important standard operating procedures, are regularly updated and maintained, especially those regarding telecommunications/ICTs.

Action Item 13: Standard operating procedures s

1. *Develop or update standard operating procedures s for emergency and disaster response related to communications within and between agencies and technical means for communication (voice/data), including interoperability.*
2. *Define the government entities and the contact points (key decision makers) within these entities that must maintain communication during a disaster or emergency.*
3. *Maintain an updated database with these focal points of every agency, and where appropriate any associated partner organizations, countries, or other external entities, involved in disaster management.*
4. *Analyse the possible interoperability between the equipment (wireless) and the communication networks of the government entities.*
5. *Establish a set of radio frequencies that can be used for the communication of the contact points (key decision-makers) compatible with the radiocommunication equipment being used and ensure it is aligned with any similar activities to ensure regional compatibility.*
6. *Establish alternative methods of communications, if necessary, for example through existing communication operators.*
7. *Develop connectivity plans for the satellite equipment available, if that is the case, to be used during a response phase as well as procedures for their use as primary or alternative communications between relevant stakeholders involved in disaster response.*

[43] United States Department of Homeland Security (2014), *National Emergency Communications Plan.*

14 Contingency plans

A contingency plan for telecommunications/ICTs must include specific procedures depending on the unique characteristics of the location, such as the level of connectivity of the site, the available facilities or equipment deployed in the area, redundancy, and power sources, among other elements.

This contingency planning, in addition, should include solutions and alternatives that can be deployed to maintain operations and communications in the affected area by the agents responsible for DRM. This should be helpful for making advance decisions on resource management, and to develop procedures for the expected use of the full range of available technical and logistical responses, especially with respect to telecommunications.

Action Item 14: Contingency planning for public and private networks

Public and private networks, including mobile, fixed and broadcasting operators must keep their contingency plans for an emergency updated. Measures such as network redundancy, mobile base stations, secondary energy sources, among others, must be considered and included in the network design, management, and maintenance plans, especially in those areas at risk according to the hazard maps and risk assessments, and considering the network vulnerability analysis. This is particularly important where there may be areas operated by independent organizations to ensure compliance with State-wide capabilities and compatibility between systems.

Other type of networks, such as satellite networks, should also be considered in the contingency plans, e.g., satellite equipment in safe warehouses, and connectivity plans for their use during the response phase of a disaster.

A process and procedure should be developed by the government agency responsible for disaster management to ensure these contingency plans are created, maintained, and verified that they are compatible with the wider policies and plans administered through that organization.

15 Early warning systems

The agencies in charge of the hazard warning within the country should be identified along with the specific hazards they protect against. Beyond the data collection capabilities within the country, the regional and global resources, and agencies upon which they rely should also be identified.

Supporting the United Nations statement that "early warning systems save lives"[44], ITU[45] has focussed on the importance of the early warning dissemination and communication pillar of multi-hazard early warning systems (MHEWS). The following elements should be considered:

1. Data gathering, analysis and dissemination: Data collection and access is a key area to ensure relevant stakeholders and decision makers are empowered to make informed decisions concerning disaster risk mitigation, preparedness, response, and recovery.
2. Human resources: DRM capability based on training, continuous improvements to the administration, and data accuracy resulting from (1.) above.
3. Technology improvement: Enabling technological improvements to support data collection and management, along with communications developments to provide better dissemination of information.
4. Education and training: Increasing public awareness and creating a more skilled and knowledgeable community, including engagement with schools, and facilitating relevant student projects.
5. Communications: Improving trust and engagement with citizens and enabling relevant and timely dissemination of DM information where both technology and education and training can contribute.
6. Legislative and policy: Ensuring the legislative and policy framework for DM continues to evolve and ensure some of the consequences of technological development need to be reflected in relevant legislation, policies, and plans.

Action Item 15: Early warning alert message dissemination

The UN executive action plan for the Early Warnings for All Initiative should be consulted and a roadmap created which demonstrates progress against this initiative which is bench marked.

The current common alerting protocol (CAP) Alerting implementation should be examined to assess its efficacy and identify opportunities for expanding its reach to as broad a number of different channels as possible. Any dependencies for downloading applications to mobile devices should be assessed for limitations in scope and coverage.

Specifically, can it propagate alerts to mobile network cell broadcast and/or location-based SMS, TV, public broadcast radio etc? Consideration should also be given to assessing interoperability between the systems operated by public service providers and private networks operated in specific designated areas. Enhancements to surveillance and monitoring systems for probable threats prior to the occurrence of disasters and/or emergencies should also be verified. With the cooperation of the telecommunication/ICT service providers, solutions to warn and alert the public could be implemented, i.e., through mobile cell broadcast technology or broadcasting networks (radio and TV). The role of Amateur radio should also be reviewed to establish opportunities for further refinement.

---

[44] World Metrological Organization (WMO) 2022. The UN Early Warning Initiative for the Implementation of Climate Adaptation: Executive Action Plan 2023-2027

[45] ITU (2023). Digital transformation and early warning systems for saving lives - Background paper

16 Drills and training

The development of an effective NETP should consider including practical strategies that improve the capacities and training of all people involved in the management of emergency telecommunications/ICTs. This is important because considering the development of these capabilities improves the speed, quality and effectiveness of emergency preparedness and response.

It is important to develop training programmes and drills particularly designed for the telecommunication/ICT sector. The development of effective training and exercise programmes can reinforce the competence of emergency services with communications equipment, as well as improve their ability to execute the policies, plans and procedures that govern the use of telecommunications/ICTs through all the process of DRM.[46]

The Emergency Telecommunications Table-top Simulation Guide, developed by ITU (2020), as well as the online training tool on How to Develop Tabletop Simulation Exercises (TTX), provide all the relevant information needed to develop and carry out this type of exercises.[47]

Action Item 16: Training and drills

Telecommunication trainings and drills for emergencies should be regularly carried out to improve emergency responder capacity with communications equipment, as well as to enhance their ability to execute policies, plans and procedures governing the use of communications networks. The telecommunication/ICT sector should actively participate in these drills and exercises, and develop and carry out their own, to effectively implement the NETP.

[46] United States Department of Homeland Security (2014), *National Emergency Communications Plan*.

[47] These documents can be consulted in the following links: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Publications/2020/TTX_Guide.pdf and https://academy.itu.int/index.php/training-courses/full-catalogue/practical-disaster-response-how-develop-table-top-simulation-exercises-ttx

17 Support for people with specific needs

Telecommunications/ICTs can also be a key tool in disaster response and management operations to reach traditionally marginalized or especially vulnerable groups before, during and after a disaster[48]. Telecommunications/ICTs can use multiple modes and channels, such as TV, radio, SMS-text messages, or the different Internet-based services and resources: video, instant messaging over the Internet, web conferencing, and social networks, among others, which all allow instant communication and sharing of photos and/or videos and satellite communications.[49]

In that sense, dissemination of disaster preparedness and planning content should be provided in multiple languages and formats. For example, subtitles can be included in visual communications so that persons with auditive difficulties could receive the message; or visual and sound alerts could be introduced in public spaces to meet the needs of as broad a swath of the population as possible.

It is important to consider incorporating the above elements into the different communication mechanisms for alerting the population about emergencies.

Action Item 17: Supporting individuals with specific needs

Working together with network operators and telecommunication/ICT service providers, governments and regulators should develop mechanisms to understand the accessibility requirements needed to guarantee that vital digital communication technologies are inclusive and therefore accessible to all persons, including people with disabilities, with specific needs, the elderly, women, and girls, as well as refugees and immigrants. This should be linked to the existing early warning systems in the country so that people receive and understand the alerts for early actions to take place.

[48] ITU (2023). Towards building inclusive digital communities
[49] Id.

Response phase

18 Communication and coordination

In the response phase, all contingency plans and standard operating procedures established in the mitigation and preparedness phases must be executed. Telecommunications/ICTs must be established to enable communications between first responders, decision makers in the government and the community.

During the disaster response phase, authorities can establish emergency operations centres or communication and coordination command posts to provide critical communications to users in each organization involved. These positions can be fixed or mobile, local, or remote, and could be located in a vehicle or in a shelter, among other possibilities.

The functions of these centres or posts are to assess the emergency, inform a dispatcher, and identify and request appropriate resources when necessary. Therefore, these command posts should be in contact with each other (one in a remote location outside the perimeter of potential danger, and the other one at the site of the emergency, for example), in order to respond to the direct requirements that are generated in the emergency area, to dispatch equipment and personnel, anticipate the need to provide more support and assistance, and position additional resources in the area.

Considering this, it is important to maintain interoperable and continuous communications between command posts and between the rest of the stakeholders involved in the response to the emergency (specially the focal point for disaster management within the country). As such, it is necessary to use all available means of communication and maintain close coordination with the various agencies involved.

SOPs and contingency plans, including temporary satellite connectivity and any other available means of communication, are particularly important when terrestrial networks are down, and key decision makers need to communicate to coordinate the emergency response.

Action Item 18: Communications for central co-ordination points

Consider planning for the development of emergency operations centres or communication and coordination command posts to provide critical communications to users in each organization involved during the response phase of a disaster. These positions can be fixed or mobile, local or remote, and could be located in a vehicle or in a shelter, among other possibilities. Maintaining interoperable and continuous communications between command posts and the rest of the stakeholders, especially the focal point for disaster management within the country, shelters and other key locations, is vital for an effective response to the emergency. The network connectivity to shelters needs to be checked to ensure it is reliable, stable, and able to cope with expected demands.

19 Collection and analysis of information

A key element during the response phase of disaster management is to develop ICT assessments to prioritize the deployment of critical ICT infrastructure to the most affected areas, and to collect and analyse information related to the immediate needs of the population affected by the emergency to manage the safe delivery of the response. Gathering and evaluating information is particularly important because this information can be communicated in a timely manner to the corresponding authorities (e.g., health entities, firefighters, civil police, among others), and to respond to the needs of the affected population as soon as possible.

For achieving this, it is necessary to use all the available telecommunication/ICT networks, and to include the collection of geospatial information from the disaster, to analyse the information obtained and coordinate the response planning geographically.

20 Emergency awareness and updates

During the response phase, it is also necessary to continue monitoring and warning of *new risks* to the affected population and to disseminate updates about the emergency.

To achieve this goal, multiple methods of communication such as sound and television broadcasting, text messages and/or audio messages through mobile operators, social networks, applications, among others, should be employed.

Call centres should be established to connect affected populations with their relatives during the response phase. Generally, these call centres can be in shelters and should use means of communication that do not congest the networks, for example, text messages. These call centres can also be established in collaboration with telecommunication/ICT operators in additional locations such as hostels and hotels.

If the country does not have the capacity (*e.g.,* equipment, human or financial resources) to establish this type of call centres, this service can be provided by international organizations, such as the UN through one of its branches. In the Central African Republic, for example, the Emergency Telecommunications Cluster established a dedicated Covid-19 call centre in the country's capital, Bangui, to give advice to callers and to refer potential cases of Covid-19 to the Ministry of Health as part of the national response to the pandemic.[50]

Action Item 19: Response phase communications and ICTs

During the response phase, call centres should be established to warn the affected population of new risks, to disseminate updates about the emergency, and to connect affected populations with their relatives. Generally, these call centres can be in shelters and should use means of communication that do not congest the networks, for example, text messages. To establish these call centres, countries could use satellite networks, that can be easily installed or seek collaboration with telecommunication/ICT operators or international organizations to establish the required telecommunication/ICT infrastructure.

[50] ETC (2020). Central African Republic – Situation Report # 37. Available at: https://www.etcluster.org/sites/default/files/documents/ETC CAR SitRep 37_July 2020.pdf

Recovery phase

21 Assessment of damage, reconstruction and improvement of telecommunication/ICT infrastructure

During the recovery phase, the damage caused to the telecommunication/ICT networks should be evaluated as a precursor to timely reconstruction and improvement of the damaged infrastructure. This reconstruction should seek, at a minimum, to restore communications to the same conditions as they were before the disaster. But preferably, ICT infrastructure should be rebuilt on the principle of *building back better*; that is, reconstructing a more resilient infrastructure that can withstand future disasters.

It is necessary to maintain the availability of a minimum level of communications for those who carry out the damage assessment and reconstruction activity and to establish communication priorities to manage available communications resources.

Action Item 20: Restoration and reconstruction

Restoration and reconstruction of the telecommunication/ICT infrastructure should be based on lessons learned and on the principle of building back better. Also, these activities should involve the active participation of the private sector, including fixed, mobile and satellite network and service providers. An essential aspect for consideration must be how the early warning can be improved as part of the reconstruction process.

22 Recovery activities follow-up

Telecommunications/ICTs must have the capacity to support the recovery activities of the affected area after the disaster. This includes continuing to transmit relevant information to, among other objectives, update the public on topics such as emergency health services, shelters, food, or family reunification.

Action Item 21: Continuing development and lessons learned

Based on the experience acquired during the disaster management, a report should be developed after the response and recovery phases identifying lessons learned and including necessary modifications and improvements that should be made to the NETP. The NETP should be updated every two to three years as a minimum and updated more frequently where there are changes in circumstances, legislation and/or regulations and policies.

Annexes: Template for collection of information

A.1 Inventory of telecommunication/ICT networks

Radio broadcasting

Company	Station name	Transmitter location (address)	Frequency (FM/AM)	Coverage (localities)

Television broadcasting

Company	Station name	Transmitter location (address)	Frequency	Coverage (localities)

Mobile providers

Mobile Provider	Coverage (District, Cities/Localities)	Technology (2G, 3G, 4G)

Fixed providers

Fixed Provider	Coverage (District, Cities/Localities)	Technology	Service

Satellite

[Satellite equipment, equipment location, voice and/or data services, satellite provider, frequencies, etc.]

Amateur Radio

[Network specifications to be provided, e.g., repeater locations, frequencies, voice and/or data service, type of equipment, etc.]

A.2 Disaster management network

[Frequencies of operation (HF, VHF, UHF, etc.), repeater locations – radio sites, inventory of mobile and portable radio terminals, callsigns, who is responsible for the equipment/network, etc. Scope and nature of the national early warning infrastructure including details of all sources of alerting information and how this is disseminated to all the different population groups, and how it is operated, managed, and maintained and most importantly – by whom.]

A.3 Private networks

[Name/owner, site locations, frequencies, coverage, etc.]

A.4 Contact information

[Contact information of key people from the government and the private sector (networks), who need to have priority in their communications in case of an emergency]

Name	Institution	Private/public	Contact information

A.5 International telecommunication/ICT support

[Contact information of key telecommunication/ICT people/international organizations for disaster relief]

Name	International organization	Contact information

A.6 Standard operating procedures

[SOPs for communications within the National Emergency Management Organization – NEMO (including the National Emergency Operation Centre -NEOC and the Director and Shelter Manager(s), among others), and between the NEMO and other bodies involved in DRM and high-level government authorities, first responders, etc. What means of communication will be used? (including wireless technology, frequencies, equipment, etc.) What are alternative means of communication?]

A.7 Contingency plans

[Summary of contingency plans from telecommunication/ICT service providers. The detailed plans are generally not made publicly available.]

References

EM-DAT: The Emergency Events Database – University Catholic De Louvain (UCL) – CRED, D. Guha-Sapir – www.emdat.be, Brussels, Belgium.

Federal Emergency Management Agency (FEMA), The Four Phases of Emergency Management.

International Telecommunication Union Development Sector (2023), Digital transformation and early warning systems for saving lives, background paper.

International Telecommunication Union Development Sector(2020), ITU Guidelines for National Emergency Telecommunication Plans.

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

United Nations Treaty Collection. Chapter XXV – Telecommunications.

Appendix: Country specific reference data

Natural Hazard Data

These tables should be used 1 when creating a country specific NETP document and updated to the latest relevant information when the editing is performed. Note that this information is obtained from a core data set known as EM-DAT: The Emergency Events Database hosted by Universite Catholique de Louvain, Belgium. This data set categorises and classifies different emergency events that have occurred over time and is useful in helping identify the hazards that must be considered in developing an NETP for a specific country. This data set contains data collected over many years, but probably the most comprehensive data of relevance to preparing NETP documents relates to the period 2000-2022 at the present time due to the consistency and reliability in this data.

Angola natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2000	Hydrological	Flood	Riverine flood	70031
2000	Hydrological	Flood	Flood (General)	6003
2000	Hydrological	Flood	Flood (General)	3001
2000	Hydrological	Flood	Flood (General)	22
2000	Biological	Epidemic	Bacterial disease	135
2000	Hydrological	Mass movement (wet)	Landslide (wet)	13
2001	Hydrological	Flood	Flood (General)	14
2001	Hydrological	Flood	Riverine flood	39976
2001	Biological	Epidemic	Bacterial disease	362
2001	Biological	Epidemic	Bacterial disease	97
2001	Climatological	Drought	Drought	58
2002	Hydrological	Flood	Riverine flood	8
2003	Hydrological	Flood	Riverine flood	609
2003	Hydrological	Flood	Riverine flood	231
2004	Hydrological	Flood	Riverine flood	331727
2004	Hydrological	Flood	Riverine flood	0
2004	Hydrological	Flood	Riverine flood	2001
2004	Biological	Epidemic	Viral disease	374
2004	Climatological	Drought	Drought	25000
2005	Hydrological	Flood	Riverine flood	10000

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2006	Hydrological	Flood	Riverine flood	225
2006	Biological	Epidemic	Bacterial disease	59924
2006	Biological	Epidemic	Bacterial disease	68
2007	Hydrological	Flood	Riverine flood	6000
2007	Hydrological	Flood	Riverine flood	40105
2007	Biological	Epidemic	Bacterial disease	18390
2007	Biological	Epidemic	Infectious disease (General)	468
2008	Hydrological	Flood	Riverine flood	81407
2008	Biological	Epidemic	Bacterial disease	7629
2009	Hydrological	Flood	Riverine flood	417
2009	Hydrological	Flood	Riverine flood	220060
2009	Biological	Epidemic	Bacterial disease	152
2009	Hydrological	Flood	Riverine flood	4650
2009	Biological	Epidemic	Bacterial disease	25902
2010	Hydrological	Flood	Riverine flood	110893
2010	Hydrological	Flood	Riverine flood	75000
2010	Hydrological	Flood	Riverine flood	3913
2011	Hydrological	Flood	Riverine flood	17
2011	Hydrological	Flood	Riverine flood	65197
2011	Hydrological	Flood	Riverine flood	5500
2011	Hydrological	Flood	Riverine flood	20100
2012	Climatological	Drought	Drought	1833900
2013	Hydrological	Flood	Riverine flood	1009
2015	Hydrological	Flood	Flash flood	2005
2015	Hydrological	Flood	Flood (General)	2001
2015	Hydrological	Flood	Flash flood	1069
2015	Biological	Epidemic	Viral disease	4983
2016	Hydrological	Flood	Flash flood	54
2016	Hydrological	Flood	Flash flood	2761

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2016	Hydrological	Flood	Flash flood	5623
2016	Hydrological	Flood	Flood (General)	1574
2017	Hydrological	Flood	Flash flood	30261
2017	Climatological	Drought	Drought	1420000
2018	Hydrological	Flood	Flash flood	3008
2018	Biological	Epidemic	Bacterial disease	141
2019	Hydrological	Flood	Flash flood	4266
2019	Hydrological	Flood	Flood (General)	1094
2019	Hydrological	Flood	Flash flood	11231
2020	Hydrological	Flood	Flood (General)	10003
2020	Hydrological	Flood	Flash flood	10630
2020	Climatological	Drought	Drought	1643316
2021	Hydrological	Flood	Flash flood	1778
2021	Hydrological	Flood	Flash flood	8181
2023	Hydrological	Flood	Flood (General)	44504
2023	Hydrological	Flood	Flood (General)	26490

Cabo Verde natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2009	Hydrological	Flood	Riverine flood	153
2004	Biological	Infestation	Locust infestation	
2009	Biological	Epidemic	Viral disease	20153
2014	Geophysical	Volcanic activity	Lava flow	2500
2002	Climatological	Drought	Drought	30000
2015	Meteorological	Storm	Tropical cyclone	9
2022	Climatological	Drought	Drought	46093
2020	Hydrological	Flood	Flood (General)	25001
2017	Climatological	Drought	Drought	70000

Equatorial Guinea natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2004	Biological	Epidemic	Infectious disease (General)	961
2023	Biological	Epidemic	Viral disease	26

Gambia natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2000	Biological	Epidemic	Bacterial disease	116
2014	Biological	Epidemic	Viral disease	
2012	Climatological	Drought	Drought	428000
2002	Climatological	Drought	Drought	
2004	Biological	Infestation	Locust infestation	
2008	Hydrological	Flood	Riverine flood	400
2009	Meteorological	Storm	Severe weather	2350
2019	Meteorological	Storm	Storm surge	15101
2015	Climatological	Drought	Drought	63100
2001	Hydrological	Flood	Flood (General)	250
2013	Hydrological	Flood	Riverine flood	3300
2021	Meteorological	Storm	Severe weather	16949
2010	Hydrological	Flood	Riverine flood	21194
2004	Meteorological	Storm	Storm (General)	6137
2007	Hydrological	Flood	Riverine flood	300
2022	Hydrological	Flood	Flood (General)	17201
2017	Hydrological	Flood	Flood (General)	20000
2010	Hydrological	Flood	Riverine flood	17767
2008	Meteorological	Storm	Severe weather	300
2003	Meteorological	Storm	Storm (General)	8019
2009	Hydrological	Flood	Riverine flood	14258

Ghana natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2001	Biological	Epidemic	Bacterial disease	733
2001	Hydrological	Flood	Riverine flood	144025
2001	Biological	Epidemic	Bacterial disease	408
2002	Hydrological	Flood	Riverine flood	200
2002	Hydrological	Flood	Riverine flood	2000
2005	Biological	Epidemic	Bacterial disease	2248
2007	Hydrological	Flood	Riverine flood	332600
2008	Hydrological	Flood	Riverine flood	58000
2009	Hydrological	Flood	Riverine flood	19755
2009	Hydrological	Flood	Riverine flood	139790
2010	Biological	Epidemic	Viral disease	100
2010	Hydrological	Flood	Riverine flood	7500
2010	Hydrological	Flood	Riverine flood	9674
2011	Hydrological	Flood	Riverine flood	12571
2011	Biological	Epidemic	Bacterial disease	10002
2011	Hydrological	Flood	Riverine flood	81473
2012	Biological	Epidemic	Bacterial disease	4975
2012	Biological	Epidemic	Viral disease	466
2013	Biological	Epidemic	Bacterial disease	560
2013	Hydrological	Flood	Riverine flood	25000
2014	Biological	Epidemic	Bacterial disease	56469
2015	Hydrological	Flood	Flood (General)	5000
2015	Biological	Epidemic	Viral disease	465
2016	Hydrological	Flood	Flood (General)	
2016	Biological	Epidemic	Bacterial disease	172
2017	Meteorological	Storm	Storm (General)	12
2017	Hydrological	Flood	Flood (General)	1000000
2018	Hydrological	Flood	Flood (General)	100000
2019	Hydrological	Flood	Flash flood	

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2019	Hydrological	Flood	Flood (General)	26102
2020	Hydrological	Flood	Flood (General)	200
2020	Hydrological	Flood	Flood (General)	
2021	Hydrological	Flood	Flood (General)	206
2021	Hydrological	Flood	Flood (General)	120
2022	Hydrological	Flood	Flood (General)	5000
2023	Hydrological	Flood	Flood (General)	250
2023	Hydrological	Flood	Flood (General)	40864

Guinea natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2000	Meteorological	Storm	Tornado	4
2000	Biological	Epidemic	Viral disease	512
2001	Biological	Epidemic	Bacterial disease	155
2001	Hydrological	Flood	Riverine flood	220009
2002	Biological	Epidemic	Bacterial disease	146
2003	Biological	Epidemic	Viral disease	67
2004	Biological	Epidemic	Bacterial disease	1192
2004	Climatological	Wildfire	Land fire (Brush, Bush, Pasture)	777
2005	Biological	Epidemic	Bacterial disease	1956
2006	Biological	Epidemic	Bacterial disease	143
2006	Biological	Epidemic	Bacterial disease	284
2006	Hydrological	Flood	Riverine flood	1200
2007	Biological	Epidemic	Bacterial disease	2500
2007	Hydrological	Flood	Riverine flood	20685
2008	Hydrological	Flood	Riverine flood	4200
2009	Hydrological	Flood	Riverine flood	40002
2010	Hydrological	Flood	Riverine flood	7622
2010	Hydrological	Flood	Riverine flood	40412

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2011	Hydrological	Flood	Riverine flood	20143
2012	Biological	Epidemic	Bacterial disease	5628
2013	Hydrological	Flood	Riverine flood	11106
2013	Biological	Epidemic	Viral disease	143
2014	Biological	Epidemic	Viral disease	6358
2015	Hydrological	Mass movement (wet)	Landslide (wet)	499
2015	Hydrological	Flood	Flood (General)	29637
2017	Biological	Epidemic	Viral disease	122
2017	Hydrological	Flood	Flood (General)	3287
2020	Hydrological	Flood	Flood (General)	49541
2021	Biological	Epidemic	Viral disease	174
2021	Hydrological	Flood	Flood (General)	71669
2022	Hydrological	Flood	Flood (General)	49536
2023	Hydrological	Flood	Flood (General)	25080

Liberia natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2005	Biological	Epidemic	Bacterial disease	674
2009	Biological	Infestation	Worms infestation	500000
2003	Biological	Epidemic	Bacterial disease	17561
2014	Biological	Epidemic	Viral disease	10682
2000	Biological	Epidemic	Bacterial disease	112
2010	Hydrological	Flood	Riverine flood	15486
2003	Biological	Epidemic	Infectious disease (General)	1857
2008	Hydrological	Flood	Riverine flood	340
2016	Hydrological	Flood	Flood (General)	15431
2009	Hydrological	Flood	Riverine flood	584
2002	Biological	Epidemic	Bacterial disease	661
2007	Hydrological	Flood	Riverine flood	17000

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2000	Biological	Epidemic	Viral disease	
2007	Meteorological	Storm	Severe weather	3500
2022	Biological	Epidemic	Viral disease	5528

Nigeria natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2000	Biological	Epidemic	Infectious disease	
2000	Biological	Epidemic	Infectious disease	40
2000	Hydrological	Flood	Flood	250
2000	Biological	Epidemic	Bacterial disease	1215
2000	Meteorological	Storm	Storm	1000
2000	Hydrological	Flood	Flood (General)	1000
2000	Hydrological	Flood	Flood (General)	750
2000	Hydrological	Flood	Flood (General)	2000
2000	Hydrological	Flood	Flash flood	500
2000	Hydrological	Flood	Flood (General)	1000
2000	Hydrological	Mass movement (wet)	Landslide (wet)	300
2000	Hydrological	Mass movement (wet)	Landslide (wet)	
2001	Biological	Epidemic	Infectious disease (General)	1
2001	Biological	Epidemic	Bacterial disease	
2001	Biological	Epidemic	Viral disease	340
2001	Hydrological	Flood	Flood (General)	2000
2001	Hydrological	Flood	Riverine flood	3852
2001	Hydrological	Flood	Flash flood	84065
2001	Biological	Epidemic	Infectious disease (General)	125
2001	Biological	Epidemic	Bacterial disease	2170
2002	Biological	Epidemic	Infectious disease (General)	2880

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2002	Biological	Epidemic	Bacterial disease	100
2002	Hydrological	Flood	Flood (General)	200
2002	Meteorological	Extreme temperature	Heat wave	
2002	Biological	Epidemic	Infectious disease (General)	750
2002	Biological	Epidemic	Viral disease	
2002	Biological	Epidemic	Infectious disease (General)	9
2002	Biological	Epidemic	Bacterial disease	164
2002	Biological	Epidemic	Infectious disease (General)	
2003	Hydrological	Flood	Riverine flood	210000
2004	Biological	Epidemic	Bacterial disease	281
2004	Hydrological	Flood	Riverine flood	1000
2004	Hydrological	Flood	Riverine flood	300
2004	Biological	Infestation	Locust infestation	
2004	Hydrological	Flood	Riverine flood	15000
2004	Hydrological	Flood	Flash flood	10600
2004	Hydrological	Flood	Flash flood	3000
2004	Biological	Epidemic	Bacterial disease	1316
2004	Biological	Epidemic	Bacterial disease	300
2005	Hydrological	Flood	Riverine flood	1000
2005	Biological	Epidemic	Infectious disease (General)	200
2005	Biological	Epidemic	Viral disease	23575
2005	Biological	Epidemic	Infectious disease (General)	
2005	Biological	Epidemic	Bacterial disease	98
2005	Hydrological	Flood	Riverine flood	3004
2006	Hydrological	Flood	Riverine flood	2000
2006	Hydrological	Flood	Flash flood	10000

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2006	Hydrological	Flood	Flash flood	1000
2007	Hydrological	Flood	Riverine flood	50000
2007	Hydrological	Flood	Flood (General)	
2007	Hydrological	Flood	Flood (General)	5000
2007	Biological	Epidemic	Viral disease	
2008	Biological	Epidemic	Bacterial disease	
2008	Biological	Epidemic	Bacterial disease	
2008	Biological	Epidemic	Infectious disease (General)	66
2009	Biological	Epidemic	Viral disease	35255
2009	Biological	Epidemic	Bacterial disease	
2009	Hydrological	Flood	Riverine flood	150000
2009	Hydrological	Flood	Riverine flood	
2010	Biological	Epidemic	Viral disease	1500
2010	Biological	Epidemic	Bacterial disease	41787
2010	Hydrological	Flood	Riverine flood	1500200
2011	Hydrological	Flood	Riverine flood	26965
2011	Hydrological	Flood	Riverine flood	950
2011	Meteorological	Storm	Lightning/Thunder-storms	12
2011	Biological	Epidemic	Bacterial disease	21382
2011	Hydrological	Flood	Riverine flood	3000
2011	Hydrological	Flood	Riverine flood	
2012	Biological	Epidemic	Viral disease	29
2012	Hydrological	Flood	Riverine flood	7000867
2012	Meteorological	Storm	Lightning/Thunder-storms	15000
2013	Hydrological	Flood	Riverine flood	81506
2014	Biological	Epidemic	Viral disease	21
2014	Hydrological	Flood	Riverine flood	10000

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2014	Biological	Epidemic	Bacterial disease	35996
2015	Biological	Epidemic	Bacterial disease	2108
2015	Hydrological	Flood	Riverine flood	100420
2016	Meteorological	Storm	Lightning/Thunder-storms	1000
2016	Hydrological	Flood	Riverine flood	12000
2016	Biological	Epidemic	Viral disease	14518
2016	Biological	Epidemic	Viral disease	914
2017	Hydrological	Flood	Flood (General)	500
2017	Biological	Epidemic	Viral disease	146
2017	Biological	Epidemic	Bacterial disease	1558
2017	Hydrological	Flood	Flood (General)	10000
2018	Biological	Epidemic	Viral disease	1081
2018	Hydrological	Flood	Flood (General)	15872
2018	Hydrological	Flood	Flood (General)	1922332
2019	Biological	Epidemic	Viral disease	22000
2019	Biological	Epidemic	Bacterial disease	665
2019	Hydrological	Flood	Flood (General)	18640
2019	Hydrological	Flood	Flood (General)	52500
2019	Biological	Epidemic	Viral disease	169
2020	Biological	Epidemic	Viral disease	365
2020	Hydrological	Flood	Flood (General)	300
2020	Hydrological	Flood	Flood (General)	
2020	Hydrological	Flood	Flood (General)	193425
2020	Biological	Epidemic	Viral disease	222
2021	Hydrological	Flood	Flood (General)	7500
2021	Biological	Epidemic	Bacterial disease	179089
2021	Hydrological	Flood	Flash flood	830
2022	Meteorological	Storm	Severe weather	1500

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2022	Biological	Epidemic	Bacterial disease	5000
2022	Hydrological	Flood	Flood (General)	2802500
2022	Climatological	Drought	Drought	19110398
2023	Biological	Epidemic	Bacterial disease	9486
2023	Hydrological	Flood	Flood (General)	1336
2023	Hydrological	Flood	Flood (General)	30000

Sierra Leone natural hazard data

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2008	Biological	Epidemic	Bacterial disease	1746
2014	Biological	Epidemic	Viral disease	14124
2000	Biological	Epidemic	Infectious disease	
2009	Hydrological	Flood	Riverine flood	1470
2010	Hydrological	Mass movement (wet)	Landslide (wet)	5
2004	Biological	Epidemic	Bacterial disease	633
2001	Biological	Epidemic	Bacterial disease	3
2019	Hydrological	Flood	Flash flood	5000
2013	Climatological	Wildfire	Wildfire (General)	2257
2022	Hydrological	Flood	Flood (General)	12982
2004	Hydrological	Flood	Riverine flood	
2019	Hydrological	Flood	Flood (General)	5381
2007	Hydrological	Flood	Riverine flood	4500
2017	Hydrological	Mass movement (wet)	Mudslide	11916
2015	Hydrological	Flood	Flood (General)	24303
2003	Biological	Epidemic	Viral disease	90
2023	Meteorological	Storm	Storm (General)	17
2011	Hydrological	Flood	Riverine flood	
2012	Biological	Epidemic	Bacterial disease	23009

(continued)

Year	Disaster Subgroup	Disaster Type	Disaster Subtype	Total # of people Affected
2005	Hydrological	Flood	Flash flood	15000
2010	Hydrological	Flood	Riverine flood	234

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

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

Office of the Deputy Director
Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

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

Digital Networks and Environment Department (DNE)
Email: bdt-dne@itu.int
Tel.: +41 22 730 5421

Digital Knowledge Society Department (DKS)
Email: bdt-dks@itu.int
Tel.: +41 22 730 5900

Projects, Partnerships and Digital Skills Department (PPS)
Email: bdt-pps@itu.int
Tel.: +41 22 730 5447

Africa

Ethiopia

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

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

Cameroon

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

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

Senegal

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

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

Zimbabwe

International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil

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

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

Barbados

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

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

Chile

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

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

Honduras

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

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

Arab States

Egypt

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

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

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 575 0055

Indonesia

International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jalan Medan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India

International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467

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

ISBN 978-92-61-42371-1

Published in Switzerland
Geneva, 2026

Photo credits: Adobe Stock