ITU Publications

International Telecommunication Union
Development Sector

Digital transformation and early warning systems for saving lives

Background paper

Digital transformation and early warning systems for saving lives

Background paper

Acknowledgements

We wish to thank Mr Benoit Vivier, Ms Charlotte Thomas, Mr Eliot Christian, Ms Elysa Jones, Mr Mark Wood, Ms Rachele Gianfranchi, Mr Ronen Daniel and Mr Peter Sanders who contributed their time and invaluable insights to this paper.

This background paper is written by Ms Vanessa Gray and Ms Amélie Grangeat (ITU). The paper is produced by the ITU's Telecommunication Development Bureau (BDT).

Disclaimers

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 secretariat of ITU 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.

ISBN

978-92-61-38191-2 (Electronic version)
978-92-61-38201-8 (EPUB version)
978-92-61-38211-7 (MOBI version)

Please consider the environment before printing this report.

Table of contents

List of figures and boxes

Figures

Boxes

Early warnings for all: a multichannel approach and the opportunities of mobile networks to reach people at risk

"Early warning systems save lives". With these words in March 2022 the Secretary-General of the United Nations, Mr António Guterres, officially announced that the UN would lead actions to ensure that by 2027 every person on Earth is protected by an emergency warning system (EWS). At the time he spoke, one-third of the world's population was not covered by this essential service, even as climate change was aggravating both the frequency of natural hazards and the need to reach and protect people at risk.

The objective of this paper is to highlight the importance of early *warning dissemination and communication*, one of the four pillars of multi-hazard early warning systems (MHEWS, see Figure 1), which ITU is leading with the newly defined executive action plan for the Early Warnings for All initiative. The key objective of the paper is to point to the opportunities offered by the growing availability and reach of communication channels, in particular mobile (cellular) networks and services, which make it possible to reach communities at risk, warn about an imminent disaster and provide people with actionable advice. The paper will highlight some key advantages of an effective emergency warning system using mobile networks. It proposes the use of cell broadcast as a minimum national early warning system. New regulations in Europe are examined to show how regulatory measures can help speed up the adoption process. An overview of legislative approaches on MHEWS adopted by 33 countries is given in the Annex, with examples of regulatory measures. It is argued that the availability, adoption, and usage of mobile network services is a critical component for the successful implementation of the ambitious Early Warnings for All initiative. The intention is to initiate discussions and drive coordination between different stakeholders: government policy-makers in emergency management, hydrometeorology and telecommunication; mobile network operators; international organizations; community organizations; and donors of international humanitarian funding. Finally, we highlight the contribution that ITU can make to capitalize on the opportunities of technology and strengthen the capacity of governments to implement and use nationwide alerting systems to save lives.

This paper thus focuses on the *warning dissemination and communication* pillar of early warning systems and on the most effective technologies for reaching and warning those at risk and guiding them to safety. It is critical to recognize the need for an overall strategy to define governance issues, stakeholders, procedures and responsibilities, to build trust within the population, and to advocate for a holistic approach of the MHEWS value cycle (Figure 1).

Figure 1: The multi-hazard early warning system value cycle. This paper focuses on the "warning dissemination and communication" pillar of the cycle

Source: WMO

An effective MHEWS reaches *everyone* at risk, *anywhere*. Only a multichannel approach, raising the alert by radio, television, billboards, mobile applications, social media, sirens etc., can properly address the diversity of communities at risk and increase the effectiveness of an alert.

The population at risk includes people in urban and remote areas, those with or without access to telecommunication networks, people with disabilities, roamers, and people speaking different languages, to name just some. The global digital transformation and digital ecosystem are creating opportunities for broadcasting alerts through new communication channels. As of 2022, 95 per cent of the world's population had access to a mobile broadband network and close to 75 per cent of the population owned a mobile phone[1]. This makes mobile networks, in combination with the ubiquitous mobile phone, an increasingly important channel for alerts. Mobile network operators (MNOs) and their infrastructure and services have thus gained enormously in importance for public warning systems (PWSs).

This paper accordingly outlines the need to cooperate with MNOs and presents concrete technical details to implement such a warning system. It discusses cell broadcast (CB), location-based short message service (LB-SMS) and the use of the Common Alerting Protocol (CAP) as an enabler of a multichannel communication approach. It makes recommendations for their adoption by other countries, especially least developed countries and small island developing States – some of the most vulnerable countries in the world.

The warning dissemination and communication part of the EWSs discussed in this paper is not limited to any particular hazard and can be applied in any emergency or in response to threat. Alerts over mobile networks have a key advantage in that MNOs have the capability to tailor coverage to a specified alerting area and user requirements, such as preferred language. In 2020, the Body of European Regulators for Electronic Communications (BEREC) published its guidelines on how to assess the effectiveness of public warning systems (2020), based on these factors: geographical and population coverage, the capacity to reach end users, support of

[1] ITU Facts and Figures 2022

inbound roamers, supported devices, supported languages, managing longer messages, steps required for the recipient to enable receiving warning messages, accessibility for end users with disabilities, reliability, geographical targeting, and scalability. Once people receive an alert, it is critical that they know which action to take. Community engagement in formulating messages is important, as are preparations and regular drills to maximize effectiveness.

While virtually all urban areas in the world are covered by a mobile broadband network, gaps remain in rural areas. In the least developed countries, 92 per cent of the population is covered by a mobile signal of some sort, but the remaining 8 per cent live in blind spots where they remain unreachable for mobile-cellular-based alerting systems. In Africa, 15 per cent of the rural population has no mobile network coverage at all, and in the Americas that figure is 22 per cent. Furthermore, coverage does not equal use. In theory, the technical capability to access a mobile network is almost universal, but significant discrepancies in uptake remain where the cost of the service or device remains unaffordable[2]. People who do not own or use a mobile phone will not receive the message except indirectly from people who do, or through other communication channels (radio, television, sirens, social media platforms).[3]

Existing inequalities, such as the digital divide and the gender gap, thus have an impact on the effectiveness of an EWS. Remedies include making access to electricity, mobile phone services and device ownership more affordable and improving digital literacy. The narrower the divide, the more people will be reached by alerts.

ITU contribution to the Early Warnings for All initiative

ITU plays an important role not only in monitoring and addressing the digital divide but also in putting the focus on the critical role of ICTs in disaster risk reduction and management. ITU supports its Member States in the four phases of disaster management through the design of national emergency telecommunication plans (NETPs), the setting up of early warning and monitoring systems, and the provision of emergency telecommunications equipment when disasters strike. As part of its work on emergency telecommunications and disaster relief, the ITU strategic plan for 2020-2023 included target 3.5: "By 2023 all countries should have a national emergency telecommunication plan as part of their national and local disaster risk reduction strategies."

ITU highlights the opportunities of using mobile networks and services and promotes national best practices from countries around the world, including the European Union (EU). It also encourages countries to consider a regulatory obligation to provide access to mobile networks and services for the implementation of a PWS and provide the appropriate incentives for their deployment. As the lead for Pillar 3, ITU will be contributing to the overall UN goal of protecting everyone with an EWS, and specifically, to do the following:

- Help reach more people over digital networks by monitoring and reducing the digital divide.
- Widely promote opportunities related to information and communication technologies and channels and last-mile connectivity for public warning systems, and publicize best practices.

---

[2] Ibid

[3] It should also be noted that the very high figures for mobile coverage refer to inhabited areas only. People outside these inhabited areas may not have access, and will not receive the mobile alert.

- Promote a regulatory approach among ITU membership/policy-makers.
- Work with the satellite industry and MNOs within its membership, and with the GSM Association (GSMA), to provide support and expertise.
- Develop technical guidelines and high-level regulatory policy to support the adoption of mobile EWS.
- Identify specific countries and experts from countries that have already implemented a mobile-cellular based EWS to support other countries interested in implementing such a system.
- Partner with other relevant stakeholders and share expertise through the CAP Helpdesk of WMO, ITU and IFRC and through ITU training and projects.
- Bring on board development agencies and international humanitarian funding donors to develop new projects delivering technical assistance.

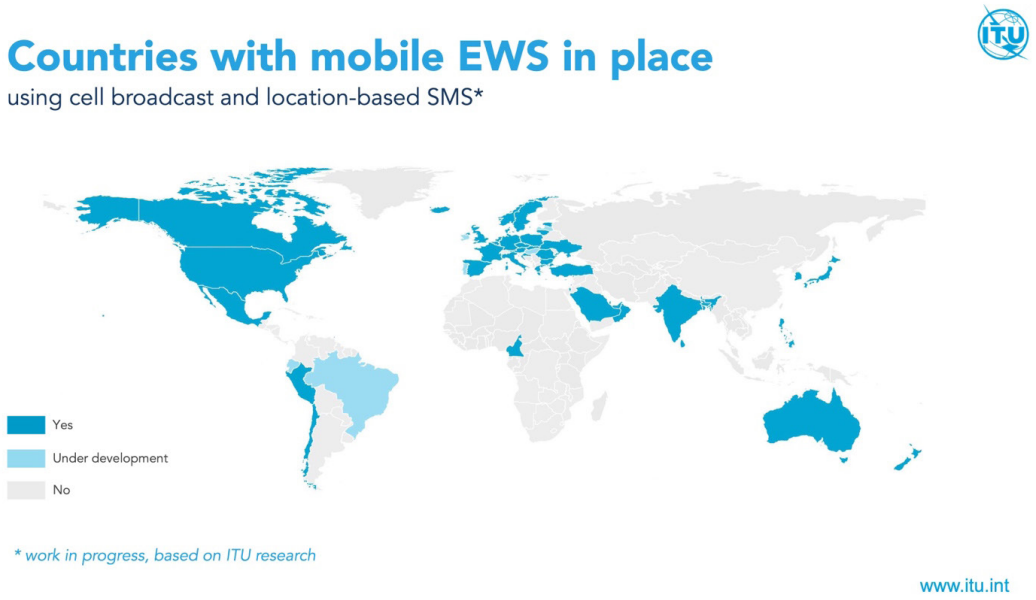
Technologies for broadcasting an alert via mobile networks

The benefits of rolling out a public warning system (PWS) based on electronic communication technology over mobile-cellular networks are multiple. First of all, a PWS can target the affected population in a specific geographical location, ensuring that messages are only delivered to those at risk so as to unduly alarming those not affected. Second, a high percentage of people can be reached, including roaming visitors from other countries. Third, messages can be sent in real time with high priority even under conditions of network congestion. Fourth, the alerting system is easy to use, and, unlike alerting systems that rely on mobile apps, does not depend on pre-installed applications or subscription.

Cell broadcast (CB) and location-based SMS (LB-SMS) are two key technologies for implementing a public warning system at the national level. Outside Europe, North America and Australia, an important illustration of their power can be found in the Philippines. When Typhoon Rai hit the country in December 2021, the national Emergency Cell Broadcast System and location-based SMS were used to reach people at risk.[4] Other countries in Asia, the Arab region and Latin America that have invested in and are developing cellular-based PWSs are Chile, Mauritius, Peru, India, Oman, the United Arab Emirates and Saudi Arabia.

[4] For a detailed description of the vital role played by MNOs during Typhoon Rai, see Typhoon Rai Response (gsma.com).

Figure 2: Countries with a mobile-based public warning system, as of August 2023



A 2013 study by the GSMA Disaster Response Group highlighted the numerous advantages of cell broadcast as the basis for a PWS. Today, CB remains the dominant technology among countries that have implemented a PWS, but there are advantages to complementing it with location-based SMS, such as embedded situational awareness. For countries with limited resources facing an urgent need to implement a basic PWS, a CB-based solution remains a recommended option.

Cell broadcast

Cell broadcast (CB) is described as follows:

"a broadcast technology operating at the default granularity of a single cell up to any size of cell group (e.g. all cells in a particular region). In this scenario the alerting gateway interacts with the CBC [cell broadcast centre] which sends a message to the destination cell…, which forwards this message over the air interface only in pre-defined time intervals until it is not needed anymore. […] All attached mobile devices connected to the cell listen for these broadcasts and display the message on the users' mobile devices where appropriate. Each warning has got its unique serial number. The mobile device remembers the serial number of the CB message, so the CB message is shown only once on each mobile device…" (2020 BEREC, PWS Guidelines).

Even mobile phones without SIM activation can receive a CB alert.

Cell broadcast technology is referred to as a point-to-N technology: a single order can trigger the broadcasting of a specific message that will be displayed on all mobile phones that are attached to the specified cells. This can be done regardless of network congestion, and at near-real-time speed, in a matter of seconds. CB allows very high precision in geographic dissemination. It is also possible to indicate the exact area of the danger/hazard, and to provide information that allows the phone to discriminate as to whether a given alert should be displayed. This type

of implementation (device-based geofencing, DBGF) also enables a geofencing technology, which means that every new person/device entering the alerting area will receive the message.

A near-real-time alert has immense benefits when a crisis affects a very large amount of people at the same time. CB is a very mature technology, standardized with the 2G GSM network, but not widely deployed, as there is little economic incentive for operators to do so. A common hindrance is the absence of a cell broadcast centre (CBC), so investment in a CBC is often the first step for CB deployment. CBCs can be established either in a decentralized way, with each MNO responsible for its own CBC, or with a centralized structure, where one CBC serves all MNOs in a country or region. The decision will depend on priorities and constraints such as cost, cybersecurity, regulation, etc. A feasibility study has been launched on a "CBC in the cloud" solution for the Caribbean islands, as a low-cost option for access to the life-saving technologies.[5]

The EU-ALERT standard adapted its CB technology to include different levels of severity, triggering different actions by the mobile handset/device. The highest priority, a national alert, is displayed on all compatible devices, regardless of the users' opt-in/opt-out status. CB also accommodates a distinctive tone that makes an incoming alert easily identifiable and communicates its urgency.

An advantage and a shortcoming at the same time of CB is that it is a blind or *one-way only* technology, providing no information on the users. This makes it possible to avoid data privacy issues, but it also means that CB does not provide any insights on what is effectively happening on the disaster scene. Those receiving the alert cannot automatically reply or otherwise contribute to rescue efforts. This lack of situational awareness also means that the CBC cannot ascertain how many mobile phone users have actually received the alerts. This is information can be crucial for the crisis management team to determine how many people are potentially affected, may need to be evacuated, etc. To give a CB-based system a degree of situational awareness, essential for crisis management, it is possible to implement complementary technologies or services such as the situational awareness component of LB-SMS technology, which can be used to build an anonymous density map. Another challenge of CB is that it is not compatible with all handsets. While most smartphones in Europe and North America are compatible, in developing and low-income countries device compatibility and alert accessibility may fluctuate, depending on the age and version of the device. A specific implementation tailored for old 2G phones may bypass this difficulty, but at the cost of dispensing with the features of classic CB reception (e.g. special alert tone or device-based geofencing).

Location-based SMS technology (LB-SMS)

A location-based SMS (LB-SMS) is a normal SMS sent to a subset of all mobile devices operating under the mobile operator network within a particular geographical area. It is thus a point-to-point technology, with the numerous advantages – and some constraints – linked to this technology.

Thus in LB-SMS mobile networks need access to a regularly updated a "last known location" database, or LKLDB, of all devices (or an MLC Mobile Location Centre), to be able to target the subset of recipients that are affected by the hazard and need to receive the alert. This information is often already existing, as MNOs need to know how to reach their end users for

[5] See World Bank (2023), Strengthening Regional Emergency Alert Capacity of the Caribbean Region.

a phone call or a standard SMS, but not necessarily in the format and the granularity needed for LB-SMS implementation. Methods for tracking the location may vary as well and are not subject to standardization. This raises the question of the coherency of implementation between different MNOs and means that some may choose an LKLDB with information on granularity of the cells, while other MNOs will calculate a more detailed location but with time used for the computation of this information.

Another issue is the location of inbound roamers, who should receive the message via LB-SMS directly, without it first going through their home networks. This will save time and increase effectiveness during an alert. Individual implementations of LB-SMS may differ for technical, political, and cost reasons, and the effectiveness of the technology may be affected by the MNO level of technical and operational experience.

Data privacy is another question that must be addressed: only if the information contained in the LKLDB stays within the MNO networks can it be considered safe. Any data extracted from the LKLDB and stored on a centralized alerting gateway should be anonymized and gathered in a way that no retro-analysis could identify a specific person's location. A common approach used by MNOs is to provide aggregate figures for the number of people per cell, or to show a density map, which is extremely helpful for crisis management situational awareness.

An important advantage of LB-SMS is that it uses standard SMS, which is compatible with all handsets and networks. MNOs can be informed about the status of the SMS sent, with confirmation of reception, and the exact number of people that have been contacted and reached. With a standard SMS it is possible to send regular alert updates during a specific time-frame (for example, 24 hours) to those who received the first message, wherever they are. This is useful if the first message was an evacuation order, for example: although those following the order will have left the area at risk, updates on the situation may be necessary. Currently, this is only possible with LB-SMS technology.

The last-known-location feature of LB-SMS technology also enhances situational awareness. It can be used to generate a population density map showing population movements, and to estimate the number of people affected by the hazard, with a breakdown by country of origin, for roamers. MNOs can also use it to generate, collect and share regular inputs of anonymized dynamic or static data to give visibility of population presence on a territory, in support of decision-making for alerting and crisis management (real-time population heatmaps on operational portals). This is important for all disaster response-related activities, and to protect not only local communities but also visitors and tourists.

One of the shortcomings of LB-SMS is that MNOs must deliver each recipient's message separately, increasing the risk of network congestion – unlike cell broadcast, which uses a dedicated channel. The speed of message delivery is also significantly reduced compared with a broadcast message. The congestion risk, and the number and speed of SMSs that operators can send depends on the MNOs' networks and market share. Even if it is possible to prioritize the sending of SMSs, network congestion is a key factor for the management of a crisis, as communication channels are critical for all emergency services.

Advantages and challenges of each technology from a crisis management perspective

BEREC lists 10 criteria for assessing the effectiveness of PWSs, listed in the table below:

- geographical and population coverage, capacity to reach end users, like geographical targeting, scalability, support of inbound roamers, supported devices, steps required for the recipient to enable receiving warning messages, supported languages, managing longer messages, accessibility for end users with disabilities, reliability of the service.

In addition to the 10 criteria by BEREC, it is also useful to add situational awareness, alert update capability, and speed of delivery, as these are essential aspects for saving lives in times of crisis. The following section will also address the issue of data privacy.

Finally, it should be noted that while this document focuses on the technologies, it is essential to consider as well the behavioural perspective, and the human factor in how authorities use available technologies, since these play a fundamental role in the effectiveness of attempts to inform the public about risks. Alerting procedures and decisions need to take into account, for example, the time of the alert, delays in the decision-making process, the frequency of alerts, time lags between alert messages, and the language used in messages.

Assessment criteria for effective public warning system: an overview

Criteria	Comment
Geographical and population coverage	On compatible **CB** devices, even phones/handsets without an active subscription (SIM card) will receive the message. **LB-SMS** coverage is identical to regular SMS coverage for a given mobile network, independent of the device. Governments need to assess the national digital divide and determine the reach of mobile networks, based on coverage and uptake, since the effectiveness of the EWS technology depends on the reach and services of the MNO (service area coverage).
Capacity to reach end users	Geographical targeting: effectiveness depends on the implementation level by the MNO side, for both technologies. The geofencing feature is the most precise technology for reaching communities at risk. With CB one message is broadcast to all devices in the area and device-based geofencing (DBGF) only prevents displaying that message when the device is outside the affected area. Scalability: there is a risk of network congestion with **LB-SMS** (which could cause delays, or non-delivery), especially when operators send a very large number of SMSs. This risk does not exist with **CB**. Visiting end users (including inbound roamers): roamers can be alerted using CB (depending on device compatibility). LB-SMS can be used to reach roamers, but special attention must be paid to the quality of the implementation of this subject on the MNO side. Supported devices: all mobile devices with a SIM support **LB-SMS**, while only compatible devices support **CB**[6]. Mobile phones without an activated SIM can receive a **CB** alert. Steps required for the recipient to enable receiving warning messages: No steps need to be taken for LB-SMS (indeed, LB-SMS does not have an opt-out option), while there are some steps to be taken for the implementation of CB: opt-in/opt-out possibilities exist in the settings of the phone (it is possible to address these with the mobile phone handset providers). For a national/executive alert there are no opt-out options. Supported languages: SMS requires that the encoding of the characters be specified. Certain **LB-SMS** implementations enable the detection of the mobile country code for inbound roamers (with data privacy restrictions), and to then send the message in the required language. **CB** enables sending multiple messages in different languages and displaying only the language of the phone menu settings. It is also possible to define a default language which will be used if the alert does not contain the user's language. Length of the alert message: it is recommended that **LB-SMS** not exceed 160 characters. It is theoretically possible to send longer text, but with a risk of losing a part of the message during the SMS broadcast. In addition, and depending on the special character used, the single message length may drop to 70 characters. **CB** supports messages with a maximum length of 1395 characters.

[6] While there is generally agreement that compatibility with CB is high, it is unclear if global of national figures exist.

Criteria	Comment
Capacity to reach end users (*continued*)	Accessibility for end users with disabilities: independent of the technology, this functionality depends on the capabilities of the device text-to-speech function. Reliability of the service: for **LB-SMS**, the reliability depends mainly on the robustness of the MNO network and service, and not on the technology itself, as is the case for any SMS. ITU regularly assesses the resilience of MNO services per country. **CB** is highly reliable in terms of network overload but is as sensitive as **LB-SMS** to network degradation in times of crisis. Alerting end users entering the area after the initial warning (geofencing): Geofencing is possible with both technologies, but **CB** is best adapted for this functionality.
Crisis management features	Situational awareness: **LB-SMS and CB**, thanks to the localization database, allows for the gathering of anonymous and valuable information for a crisis. This includes the number of GSM users in the areas of danger (which helps estimate the number of people affected), the density of GSM users/mobile devices (for example, to estimate the danger of a panic). In addition, in the case of SMS, it is possible to confirm how many people received the SMS, and for authorities to confirm that people at risk have received the alert message on time. This data should be anonymized, and not include individualized personal data, for privacy reasons. **CB** is a "blind technology", without situational awareness, that does not offer the above information. However, it should be noted that it is possible to set up an interactive CB function, with situational awareness functionality that allows users to respond to an alert. Alert update capability: alert messages are especially useful in two situations: "Take shelter" and "Evacuate". For the "shelter" order, since people are not moving, both technologies can send updates based on localization. In the case of the "evacuate" order, most people will leave the affected area. In this case, **CB** cannot provide evacuees with updates. Depending on the implementation, **LB-SMS** can provide this service using the original list of recipients. This is useful for updates and for an "All clear", for example. Speed of delivery: **CB** is a near real-time technology, independent of the recipient's number. **LB-SMS** speed depends on the network level of congestion and the quality of its implementation. Optimizations are necessary to make sure that the speed of delivery meets the need. For local crises, both technologies are suitable. If the situation concerns a very large number of people, or requires delivery within seconds (e.g. an earthquake warning), **CB** is the only technology that will be able to deliver alerts on time. Data privacy: CB is a blind technology, so compliance with data privacy rules such as the EU's General Data Protection Regulation (GDPR) is not an issue. LB-SMS is compliant under the condition that individual personal data are not communicated outside the MNOs' servers, even for situational awareness (protection required at the level of the implementation).

In conclusion, CB and LB-SMS technologies both have advantages and disadvantages and can complement each other in the management of an emergency. In general, the near-real-time speed of CB makes it attractive for the response to national crises (rare, but major events). LB-SMS is attractive for crisis management at a more limited, local scale (more frequent, more localized), as it supports updating, ensuring that all targeted devices have been reached, and providing situational awareness. The 2020 BEREC study cited above reports that a survey on public warning systems showed that 80-98 per cent of alerts in Europe were sent to up to 50 000 end users. At this scale, the two technologies are equivalent in terms of speed. Some countries,

like France and Australia, have chosen to implement both technologies in parallel, recognizing their complementarity in crisis management. For countries with more limited budgets and MNO networks of varying maturity having to choose one technology, CB is usually the recommended choice.

This choice of technology also reflects a number of challenges at the governance level of a multi-hazard emergency warning systems that need to be addressed prior to implementation:

- Potential opposition from the MNOs, as there is no business model and no financial incentive for them to make their networks available for the purposes of an EWS. This is usually overcome with governments (or donors) providing the appropriate funding for what can be considered a public good.[7] An adequate legal framework could also help to guide this cooperation, addressed later in this paper.
- The cost of such a system, which depends on the technical choice and the MNO technical maturity. Since CB is standardized, the technology is usually less expensive to implement and maintain on 4G/5G networks compared to LB-SMS. A CB message is free for the user by default. By contrast, if an LB-SMS alert is to remain free of cost for the end user, that will require regulatory measures, adding complexity to the project. The cost is particularly challenging for highly fragmented markets, such as island nations in the Caribbean: here, any given MNO typically has only a few cell towers, and revenues are unlikely to justify the expense of establishing a physical CBC. However, with a return on investment estimated at 23 to 35 per cent per year[8], experts agree that in countries heavily exposed to climate risk, including SIDS and cyclone-risk prone countries, the cost of a MHEWS is rapidly recovered in terms of lives, livelihood and livestock saved. According to one study, the impact on gross domestic product (GDP) of such climate disasters has set back the economic development trajectory of some countries by up to a decade, with cyclone-induced disasters alone amounting to a mean annual global loss of USD 16.7 billion.[9]
- Privacy and data security issues, which need to be addressed in implementation. The population needs to be confident that their personal data is safe and will not be misused, and that the technology intended to provide tailored life-saving information is not misused for undue profiling and tracking of individuals. Any public warning system will need to comply with the strictest national privacy and security regulations and communicate transparently with the population.
- Respect for confidential internal MNO information – such as the technology used – in the architecture of the implementation of the MHEWS, as MNOs are in competition with each other.
- Authorization structures within the crisis management system and structure. The system needs to clearly identify the authority and responsibility of different stakeholders. This includes identifying who is authorized to send specific alerts, for different events and via different stakeholders. This includes designing, adopting and enforcing operational procedures and best practices for the chain of command and alert validation, to manage the human factor in using the alerting system.
- It should also be noted that while mobile-based EWSs have considerable advantages, in particular their reach, they become vulnerable in the aftermath of a disaster, as the damage sustained can drastically degrade their capabilities. In this case, radio broadcasts and satellite-based alert system, such as the one currently under development by the European Commission, provide redundance and resilience (Box 1).

---

7 Gray and Gianfranchi (2023), Resilience to climate change: telecom networks and software for early warnings for all, available at https://www.everbridge.com/customers/success-center/resource/public-early-warning-systems-for-all/

8 See Alliance for Hydromet Development(2021), Hydromet Gap Report 2021

9 Kunze, Sven (2021), Unraveling the Effects of Tropical Cyclones on Economic Sectors Worldwide: Direct and Indirect Impacts, https://link.springer.com/article/10.1007/s10640-021-00541-5 accessed 23/08/23

Box 1: Alerts via satellite – Galileo Stellar project

From 2025, Galileo, the European global navigation satellite system (GNSS), will provide a **contribution to early warning systems** through a new service called Galileo Emergency Warning Satellite Service (EWSS). This satellite service, free of charge to users, will broadcast **warning messages to populations threatened by natural disasters or other emergencies in affected areas.** Galileo receivers implemented in various devices (e.g. smartphones, handhelds, billboards, etc.) could receive, decode and display these messages. The service will be independent of terrestrial communication networks and will be provided even when such networks are unavailable.

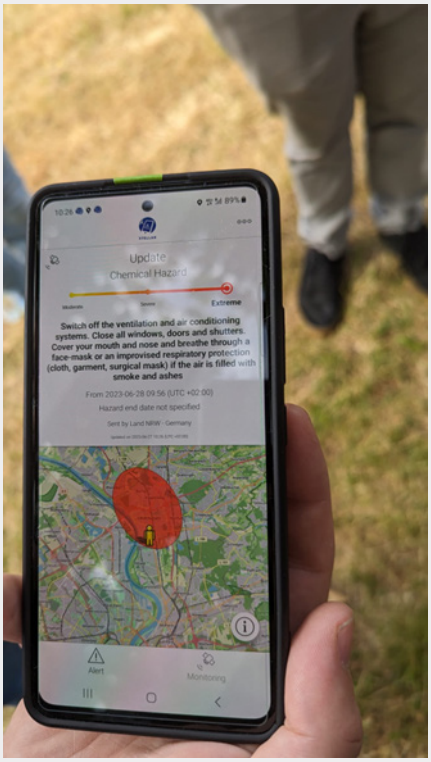
Following a preliminary demonstration phase of the service in France, Italy and Australia, EU member States decided in 2021 to establish a new satellite-based service for alert dissemination to the population, by making use of the advantages offered by Galileo. This new emergency warning service, which was officially established in article 45 of Regulation (EU) 2021/696 establishing the Union Space Programme, is currently being implemented in the Galileo system. The principle is that the satellite dissemination capacity is put at the disposal of national civil protection authorities, for the purpose of alerting their citizens in case they are threatened by a looming disaster in any given area.

Currently, the STELLAR project, funded under the EU programme Horizon Europe, continues to engage with civil protection authorities to perform multiple in-field demonstrations of end-to-end delivery of emergency warning messages across Europe. Alert messages are acquired from the Galileo signals and displayed on the screen of a mobile phone. The system is independent of MNOs so it functions even if mobile services become congested or collapse, and covers areas that lack network coverage (open sea, desertic areas, mountains). The service is not intended to replace other alert systems, and it has some limitations: satellite signals are unlikely to be received indoors, and free-text messages with customized guidance are not possible.

Figure 3: How to alert the population via Galileo (*EENA, 2022 CAP Workshop*)

The results of the in-field demonstrations show the complementarity between the dissemination of alert by satellite navigation systems and by CB or LB-SMS. The content of the alert message that is transmitted to Galileo for broadcast is formatted using the Common Alerting Protocol (CAP), described below). Alerts are matched to a predefined list of alerts (text) and then decoded by the user device so that the user is notified. A library of predefined instructions is available and encoded in the alert message to provide information to the user. The dissemination service can be easily integrated into existing operational practices and systems for population warning.

Figure 4: Picture of a smartphone receiving a test alert via Galileo, during the Stellar demonstration conducted in Leverkusen (Germany) in 2023



In summary, with a global capacity, independent from terrestrial mobile networks, and free of charge to end users, satellite navigation systems present a great potential for future crisis management.

Standardizing alerting messages: the Common Alerting Protocol

MHEWS are more efficient with a multichannel approach, which means disseminating an alert via different communication networks with a consistency among the different channels used. A cellular based EWS should be the minimum objective, making it possible to reach the vast majority of people at a relatively low cost per capita. However, countries should consider other channels – radio, TV, sirens, satellite, pushed messages via mobile applications, digital

billboards, etc. – as possible options, taking into account their exposure to risk, population density profiles and infrastructure coverage.

Whatever the channel, ITU recommends the use of the Common Alerting Protocol (CAP), which is a simple, general format for exchanging all-hazard emergency alerts and public warning information over all kinds of networks, communicating key facts of an emergency, such as the description of the emergency, instructions, the alerting area, and the urgency, certainty and severity of the alert. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. Adopted by the International Telecommunication Union as Recommendation ITU-T X.1303bis[10], "it provides both an XML schema definition (XSD) specification and an equivalent ASN.1 specification (which permits a compact binary encoding) and allows the use of abstract syntax notation one (ASN.1) as well as XSD tools for the generation and processing of CAP messages." This Recommendation is technically equivalent to the OASIS Common Alerting Protocol v.1.2. and the structure is compliant with other existing formats, including the Specific Area Message Encoding (SAME) protocol used on the weather radio network of the National Oceanic and Atmospheric Administration (NOAA) in the United States and the national Emergency Alert System (EAS).

ITU and other institutions train countries on the use of CAP for exchanging all-hazard emergency alerts and public warnings over all kinds of ICT networks, to ensure interoperability between the MHEWS control centre and different media.

An international standard, CAP provides for:

- Interoperability of alerts among all kinds of emergency information systems
- Message completeness, for an effective public warning
- Simple implementation
- Simple XML and a portable structure, sufficiently abstract to be adaptable to non-XML coding schemes
- Multi-use format, with one message schema supporting multiple message types in various applications
- Clarity/familiarity, so that code values are meaningful to non-expert recipients

The worldwide usage of CAP and its evolution

Together with the World Meteorological Organisation (WMO), the United Nations Office for Disaster Risk Reduction (UNDRR) and the International Federation of Red Cross and Red Crescent Societies (IFRC), ITU is active in promoting CAP, sharing CAP knowledge[11], gathering the community of users and promoting interoperability for improving alert coverage.

Today, over 75 per cent of the world's population lives in a country with at least one national operational CAP feed[12] (see Figure 5). Many of the world's most vulnerable countries, especially the least developed countries and the small island developing States, do not yet use CAP.

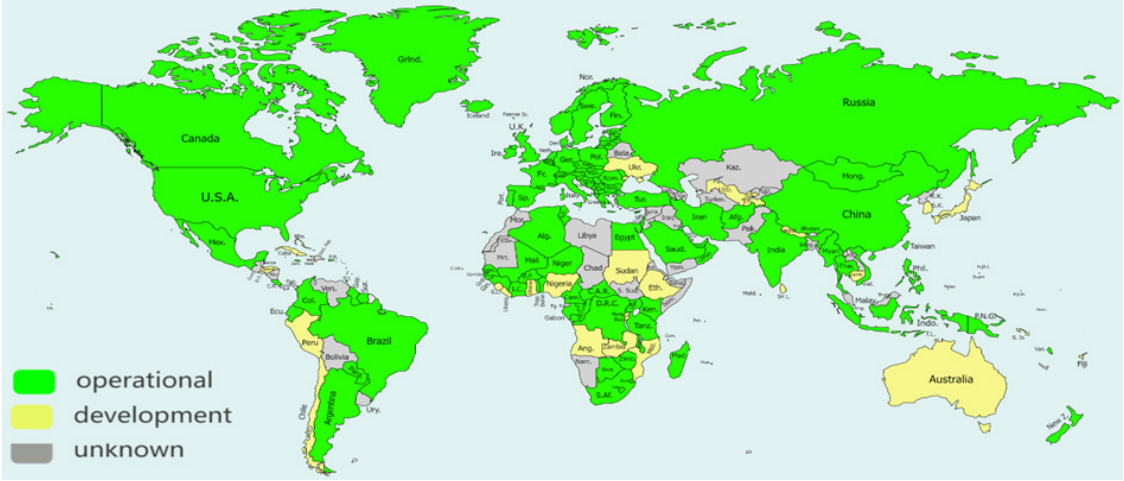
[10] Available at: https://www.itu.int/rec/T-REC-X.1303bis-201403-I

[11] Guidelines for Implementation of Common Alerting Protocol (CAP)-Enabled Emergency Alerting https://etrp.wmo.int/pluginfile.php/17980/mod_resource/content/1/wmo_1109_en.pdf

[12] See https://cap-workshop.alert-hub.org/2022/flyer.pdf

In 2021 ITU, IFRC and WMO, endorsed a call to action which recommends that "by 2025 all countries have the capability for effective, authoritative emergency alerting that leverages the Common Alerting Protocol".

Figure 5: Countries with at least one operational CAP feed, September 2022



The Alert-Hub website[13] aggregates real-time CAP alerts from 184 sources in 188 countries. As CAP is an open standard, everyone can push a CAP feed. To provide a documented basis for establishing the credibility of official CAP alerts, WMO and ITU have established an international register of alerting authorities[14].

How countries are adapting CAP to their needs and use

To implement CAP, adaptations are necessary to address the needs of different alerting authorities, as well as the technical constraints of different alerting systems. For instance, with a location-based SMS, it is recommended to limit the length of the message to 160 GSM7 characters. Cell broadcast has its own international protocol of implementation,[15] established by the 3rd Generation Partnership Project (3GPP) after the European Telecommunications Standards Institute (ETSI) standard more than 20 years ago. Using CAP with the CB standard requires a number of specifications, for example on how to send a CAP alert including the geofencing CB option. The interpretation of an area description is also subject to caution: if the CAP alert specifies a geographic location (defined by a polygon), MNOs need to know if they should trigger only the antennas situated within the polygon, or also antennas outside the polygon, but with coverage extending partly into the area of danger. The interpretation of all area fields should be homogeneous between MNOs and needs to be specified. This includes the interpretation of a CAP update order or cancel order and must be detailed through a general agreement between national authorities and MNOs.

---

13 See Filtered Alert Hub: Introduction available at https://www.alert-hub.org

14 For more information, see Register of WMO Members Alerting Authorities

15 ETSI TS 123 041 V15.3.0 (2018-09) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041 version 15.3.0 Release 15)

These additional restrictions and rules lead to local CAP versions. To ensure that interoperability between countries/actors/media is maintained despite this diversity, a "CAP translator" is required that tracks the differences between the CAP versions developed by each authority. To this end, alerting authorities are encouraged to publish the description of their CAP version.

A Common Alerting Protocol Helpdesk, currently under development, promises to help ensure coherence between stakeholders' needs and the technical constraints. In any case, communication and community-building around CAP is essential. Despite local adaptations, with CAP, every alerting authority speaks the same language, enabling communities to exchange alerts more efficiently.

A multistakeholder approach to building an effective early warning system

As shown above, building an effective public early warning system not only involves technological choices but also requires stakeholders to come and work together. A regulatory approach and framework that governs and outlines the roles and responsibilities of different stakeholders can help drive and speed up implementation and allow governments to optimize the use of existing telecommunication channels and networks to reach communities at risk and save lives. The involvement of MNOs offers great opportunities for complementing existing public warning systems and building new ones, and for advancing their deployment around the world. Discussing these opportunities and identifying different approaches for cooperation will require MNOs, the GSM Association (GSMA, the global association of mobile operators) and national policy-makers, in particular telecommunication regulators, to cooperate. Here, ITU has an essential advisory role to play, including by encouraging national telecom regulators to consider a regulatory approach.

Existing research and examples show that legislative frameworks regulating the deployment of multi-hazard early warning systems (MHEWS), and mobile EWSs in particular, depend on the existing governance structure and role of stakeholders, as well as on the role of the government in driving the set-up of a PWS. Countries may use this document, and the information provided in the Annex, as guidance on the different approaches to optimizing cooperation and coordination of all actors.

In addition, ITU can help with coordination and cooperation in the following areas:

- Bringing more people online and addressing the digital divide, in line with ITU mandate. This includes the development of networks and infrastructure, but also addressing the digital skills and affordability gaps, helping to reduce digital inequalities and allow more people to be reached in times of disasters.
- Improving the resilience of telecommunication networks, including those of MNOs, for example through the development of national emergency telecommunication plans (NETPs) to ensure the availability of services in times of crisis.
- Supporting developing countries in particular in implementing the CAP, as well as cell broadcast/location-based SMS technology, to make sure that communication between alerting authorities and MNOs is coherent and effective. As alerts may be considered public information, CAP alerts should be published on a public governmental feed, so that other media can rebroadcast the alert via other channels.
- Helping to promote best practices in setting up EWSs via mobile networks, using various ITU platforms, meetings, diverse membership and existing partnerships and building

on the experience of EU countries with the technical and the regulatory aspects of EWS adoption, but also that of countries in Latin America, Asia and Africa that have already adopted EWSs.

- Identifying best practices, sharing experiences, and encouraging specific countries and experts with experience in public warning systems to provide implementation support.
- In partnership with WMO, IFRC, GSMA etc., encouraging development agencies and donors to invest in developing mobile-network-based EWSs and set up a global project to provide technical assistance to countries. This could be an important step towards a broader and global risk management approach and achieving the UN goal of ensuring that by 2027 everyone is protected by an EWS.

Opportunities in the regulation of public warning systems: the EU example

As part of its promotion of best practices, ITU has analysed in depth the case of Europe and its regulatory action mandating countries to adopt a PWS based on mobile-cellular networks.

In 2018, a public warning system based on telecommunications was added to the European law, through the European Electronic Communications Code (EECC). EECC article 110[16] required member States by 21 June 2022 to "ensure that, when PWSs intended for imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned." The term "end-users" means every person located within an area of danger, including roamers and those without a prior subscription to any specific alerting service. To help countries in their technology choice, BEREC published its guidelines on how to assess the effectiveness of a PWS (2020).

By mid-2023, almost all European countries had either adopted such a PWS, or were in the selection process to develop the system. The European path and experience are likely to produce many lessons learned, both in terms of the technologies adopted and in terms of the regulatory approach. It will also help to understand how its technological and regulatory approach could help speed up the deployment of public warning systems in other parts of the world, and to help achieve the goal of an EWS for all. It is important to note that the success of a public EWS does not depend only on the technological implementation; it needs to be based on a holistic strategy that includes the full integration of each of the pillars of the MHEWS value cycle (see Figure 1 above). Some of the lessons from the European experience have been summarized in Box 2. However, the particular circumstances and needs of countries with limited resources will have to be taken into consideration.

[16] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

Box 2: A European perspective: eight recommendations to get the most out of a public warning system

To build an effective EWS, there are a number of lessons to be learned from the Europe regulatory and technological path:

1. Use both cell broadcast (CB) and location-based SMS (LB-SMS): the two technologies have different advantages and shortcomings, so a combination of both may be an ideal solution, FOR countries that have the necessary financial resources and expertise.
2. Combine CB and LB-SMS with other technologies and channels, including mobile alerting apps, social media, sirens, billboards etc. A multichannel MHEWS is critical to reach as many people at risk as possible.
3. Use PWS for better situational awareness, to give emergency services critical information on those at risk, including the number of subscribers within a risk zone, and allow national authorities to perfect their disaster response.
4. Define a usage strategy in advance. For the public EWS to be successful, it is important to identify risks and appropriate scenarios, addressing such question as: Who will send the alert? What message should be sent, requiring which kind of action? Which area should be alerted and which communication channels should be used?
5. Prepare standardized messages, based on the identification of risks and the communities that may need to be reached, so that in case of an emergency, messages can be sent without delay. This should be done involving the communities during the testing phase.
6. Make use of allies: they can complement and/or improve the system. Allies can be found among researchers, influencers, local volunteers and members of the general public.
7. Keep a coherent message across the different channels to avoid confusion and reinforce the message sent. The use of CAP is critical in this regard.
8. Prepare the population and increase their trust through regular tests and awareness-raising campaigns.
9. Develop a unified interface towards smartphone operating systems, so that national authorities don't have to approach the companies separately.

Source: adapted from EENA blog by Benoit Vivier

It should be noted that the regulatory approach adopted by the EU has been adopted in other regions. In Peru, for instance, the 2016 PWS regulation aims at "guiding the population, […] before, during and after the occurrence of a disaster or an emergency situation, using […] public telecommunications networks and services".[17] In the Philippines, the Free Mobile Disaster Alert Act of 2014 mandates telecommunication operators to issue free public warnings via mobile phones[18]. Regulation is an effective way to implement a public warning system. At the same time, any approach must include discussion with the MNOs, who as (generally) private companies, need to understand financial implications and ensure their business continuity. In addition to delivering humanitarian assistance and saving lives, it is therefore possible to discuss other financial and non-financial incentives to drive cooperation.

[17] LAW N°30472 on the Creation of SISMATE, and Decreto Supremo n°019-2016-MTC about the creation of SISMATE project ("Sistema de Mensajería de Alerta Temprana de Emergencias", translated in "Emergency Early Warning Messaging System")

[18] PHIVOLC or PAGASA (GoP, 2014). See www.unisdr.org/files/68265_682308philippinesdrmstatusreport.pdf (unisdr.org)

Conclusion

Early warning systems save lives and improve the resilience of societies, which is vital in a world increasingly threatened by extreme weather events and other emergencies. Growing digital transformation and increased access to and use of mobile networks and services offer new opportunities for building effective and wide-reaching early warning systems. This paper argues that to achieve the UN goal of protecting every person on Earth with an EWS it will be imperative to take advantage of the reach of MNOs to deliver warning messages to communities at risk. It highlights the possibilities of mobile-network-based PWSs, discusses two key technologies, cell broadcast and location-based SMS, and outlines the use of CAP for implementation. While there are advantages to combining CB and LB-SMS, countries at risk with an urgent need for a basic PWS may wish to consider implementing CB first.

The paper has made the argument for a regulatory approach similar to the one adopted in the EU and highlighted the need to overcome the digital divide for more effective EWS and the importance of cooperation and coordination among key stakeholders, including MNOs, disaster management agencies and policy-makers. It has shown the importance of multistakeholder engagement and highlighted the role of ITU in promoting and strengthening a global mobile-network-based EWS. This includes partnering with key international and regional stakeholders to identify best practices, delivering technical assistance, and identifying financing models to implement the system in the world's most vulnerable countries, where EWSs remain weak.

References

Alliance for Hydromet Development (2021). Hydromet gap report 2021, available at: https://www.preventionweb.net/publication/hydromet-gap-report-2021

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

European Emergency Number Association (2019). Public Warning Systems update, available at: https://eena.org/wp-content/uploads/2021_02_18_PWS_Document_FINAL_Compressed.pdf

European Emergency Number Association (2018). Public Warning in Chile, available at: https://eena.org/knowledge-hub/documents/public-warning-in-chile-resilient-culture/?_rt=MXwxfGNoaWxlfDE2ODEyMDAwMjg&_rt_nonce=72af6ed380

European Telecommunications Standards Institute (2018). ETSI TS 123 041 V15.3.0 (2018-09) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041 version 15.3.0 Release 15), available at https://www.etsi.org/deliver/etsi_ts/123000_123099/123041/15.03.00_60/ts_123041v150300p.pdf

Gray, V. and Gianfranchi, R. (2023). Resilience to climate change: telecom networks and software for early warnings for all, available at: https://www.everbridge.com/customers/success-center/resource/public-early-warning-systems-for-all/

Kunze, Sven (2021). Unraveling the Effects of Tropical Cyclones on Economic Sectors Worldwide: Direct and Indirect Impacts, https://link.springer.com/article/10.1007/s10640-021-00541-5 accessed 23/08/23

GSMA (2022). Typhoon Rai Response, available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/03/Typhoon-Rai-Response_Final.pdf

International Telecommunication Union (2022). Measuring digital development: Facts and Figures 2022, available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

International Telecommunication Union (2014). Recommendation ITU-T X.1303bis, available at: https://www.itu.int/rec/T-REC-X.1303bis-201403-I

OASIS Open (2023). Mobile Alerting Practices Version 1.0, available at:https://docs.oasis-open.org/emergency/mapcn/v1.0/cn01/mapcn-v1.0-cn01.pdf

The Body of European Regulators for Electronic Communications (2022). BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means, available at: 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

World Bank report (2023). Strengthening Regional Emergency Alert Capacity of the Caribbean Region

World Meteorological Organization (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#.Y5McJC-B1pQ

World Meteorological Organization (2013). Guidelines for Implementation of Common Alerting Protocol (CAP)-Enabled Emergency Alerting, available at https://etrp.wmo.int/pluginfile.php/17980/mod_resource/content/1/wmo_1109_en.pdf

Annex 1: Multi-hazard early warning systems: legislative approaches around the world

In March 2022, the United Nations Secretary-General António Guterres launched the Early Warnings for All (EW4A) Initiative, which stipulates that by 2027, every person in the world should be protected by an EWS (EWS).

The maturity of EWSs across countries varies widely, as do national approaches to ensure that they are implemented and operational. Recognizing the importance of this tool for climate adaptation, many countries have put in place a legislative framework that governs the roles and responsibilities of different stakeholders involved in disaster and crisis management.

This Annex provides a partial overview of national legislation that specifically refers to the use of telecommunication networks and services for early warning, and particularly mobile EWSs, to reach communities at risk. This is in line with the mandate given to ITU, which leads (with support from IDRC, WMO, UNDP and REAP) the EW4ALL Pillar 3 on *Warning Dissemination and Communication,* for last-mile connectivity to ensure that warnings reach the people at risk in time to take action (see Figure 1 on p. 2). It also aligns with the EW4All Action Plan launched during COP 27, which calls for the promotion and implementation of geolocated mobile-based early warning services using cell broadcast and/or location-based SMS, as a critical element for warning dissemination and communication. Within the broad, multichannel approach promoted by ITU, which aims to use all communication channels, mobile EWSs are a particularly powerful and promising solution, given that most people in the world are covered by a mobile network, and three out of four people own a mobile phone. It also highlights the important role of mobile network operators (MNOs) in cooperating and in opening up their networks to allow governments to broadcast alerts.

Experience from countries that have adopted a regulatory approach shows that it can be a very effective way of speeding up the process of bringing together different stakeholders, identifying roles and responsibilities and generally speeding up implementation. The legislation and regulations set out in this Annex preceded and/or accompanied the implementation of EWS. It can be seen that countries have developed different legislative approaches in accordance with their governance structure. The list is not exhaustive; other countries have also taken a legislative approach, for example the Philippines[19] and Indonesia[20] (although the latter does not specifically refer to cell broadcast, or location-based SMS).

Structure of the overview on legislation/regulation

This Annex provides an overview of public warning legislation for 33 countries, and spells out differences and similarities in terms of the governance structure, the role and responsibilities of

[19] See Republic Act No. 10639 of June 2014, "Act mandating the telecommunications service providers to send free mobile alerts in the event of natural and man-made disasters and calamities".

[20] After the 2004 tsunami Indonesia created Ina TEWS (Indonesian Tsunami Early Warning System), and then Ina-MEWS (Indonesia-Meteorological Early Warning System), and finally Ina-CEWS (Indonesia-Climate Early Warning System). The initial legislation for these early warning systems is in Indonesian law no. 24/2007 on disaster management. Law 31 of 2009 on meteorology, climatology and geophysics which defines the responsibility of the Agency for Meteorology, Climatology and Geophysics (BMKG) as a leading institution in the upstream area of early warning systems (source: CABARET report on Indonesian MHEWS). Recently, Regulation 93/2019 ("Strengthening and Development of Earthquake Information Systems and Tsunami Early Warning") mentioned "dissemination activities", but without mentioning cell broadcast or LB-SMS.

the alerting authorities, reference to specific legislation, and the role of the Common Alerting Protocol (CAP).

The implementation of a multi-hazard early warning system (MHEWS) may rely on two different types of regulation/legislation that will be identified for the examples below. These laws and regulations relating to the institution overseeing a country's crisis management regulate alerts issued by the alerting authority. Alerting authorities have the responsibility to trigger and use specific systems for warning their population. The organization of this system depends on national governance systems. In some cases, different hazards fall within the responsibility of separate authorities, so the legislation and frameworks for these hazards are separate. These specificities are presented in the following two points of the tables:

- *Governance* concerns the structure of the country (e.g. federal or centralized) and the laws that apply in terms of crisis management responsibilities.
- *Different alerting authorities* indicates if different hazard categories are under the responsibility of a single authority or several.

In some cases, a separate institution may oversee the implementation of an alerting system, with details on the specifications and the timeline of these implementations presented:

- The mandated institution in charge of establishing the emergency warning system is identified.

The table also makes reference to specific legislation on the publishing/issuing alerts. In the context of this Annex, which focuses on mobile EWSs, the emphasis is on specific language that refers to the use of existing telecommunication networks and technologies mainly in the telecommunication industry, and with reference to cell broadcast, location-based SMS. In the near future, satellite systems are likely to be used.

- The legislation on the publishers of alerts, with a specific focus on (MNOs).

Finally, information is provided on the use of CAP[21] , a simple and general format for exchanging all-hazard emergency alerts over all kinds of networks. An explicit reference to the use of CAP promotes alert interoperability and effectiveness of the multichannel approach, which also applies for private initiatives that rebroadcast alerts for the protection of the users of private services.

- CAP adoption is referenced, with an indication of the documents (legislations, technical specifications) where the protocol is mentioned.

Countries included

This overview covers 33 countries: Australia, Canada, Chile, member States of the EU (27 countries)[22], USA, Philippines and Indonesia[23]. The information in the tables below is thus only

[21] CAP as been adopted as ITU-T Recommendation X.1303. It is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of ICT networks, allowing a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task.

[22] EU countries include : Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden

a partial overview: other countries may have adopted other legislative approaches. Sources of legislation and regulations are shown in the list of references at the end of the Annex.

Australia

Governance	Federation: States and Territory governments have primary responsibility for emergency communications and warning systems within their jurisdictions: - State Emergency and Rescue Management Act 1989 (NSW); - Emergency Management Act 1986 (Vic); - Disaster Management Act 2003 (Qld); - Emergency Management Act 2005 (WA); - Emergency Management Act 2004 (SA); - Emergency Management Act 2006 (Tas); - Emergencies Act 2004 (ACT); - Northern Territory Disasters Act 1979; - RCN.900.116.0023 – Commonwealth Attorney-General Department, 'Australia's Emergency Warning Arrangements' (April 2013).
Different alerting authorities for different hazard?	Yes. "Under the authority of the Meteorology Act 1955, the Bureau of Meteorology disseminates warnings, watches and advices on weather events such as severe thunderstorms, fire weather, coastal hazards, high winds, flood and tropical cyclone warnings and, in collaboration with Geoscience Australia, tsunami warnings" RCN.900.116.0023.
Who is in charge of establishing the Emergency Alerting System?	Federal state. The Victorian Government, through Emergency Management Victoria (EMV) administers EA on behalf of all Australian governments and manages the partnership with Telstra, Optus and Vodafone to deliver this service on behalf of all Australian governments. HAF.9002.0001.0020.
Legislation on warning republishers and MNOs	While there is no legislative requirement for broadcasters to undertake the role of warning communities, there is a strong public expectation that broadcasters will disseminate warnings under section 123 of the Broadcasting Services Act 1992 (Cth), broadcasters such as MNOs have developed codes of practice in consultation with the Australian Communications Media Authority (ACMA). "Code of Practice for Warning Republishers" 2013 that covers MNOs: "Republishers are encouraged to consider the following standards (to the extent that they are relevant and within the control of republishers), which are recognised by government authorities responsible for issuing emergency warnings to the public " including the CAP conformity.
CAP reference	Yes. The "Code of Practice for Warning Republishers" 2013 mentions the compliance with the Australian Government standard for Common Alerting Protocol - Australia Profile.

Canada

Governance	Federation: "A government institution may not respond to a provincial emergency unless the government of the province requests assistance or there is an agreement with the province that requires or permits the assistance. " Emergency Management Act, 2007
Different alerting authorities for different hazard?	Yes. Only official "Authorized Government Agencies" can send alerts. It concerns: - Environment Canada for meteorological alerts such as artic outflow, blizzard, blowing snow, flash free, fog, freezing drizzle, freezing rain, snowfall, special marine information, weather, wind, winter storm, etc… - Federal/Provincial/Territorial authorities for the other types of alerts
Who is in charge of establishing the Emergency Alerting System?	In 2007, the Canadian Radio-television and Telecommunications Commission (CRTC) issued a public notice that it would take a voluntary approach for radio and television broadcasters toward distribution of public alerts. It is then followed by a Public Private Partnership in 2009: "In accordance with Canadian Radio-television and Telecommunications Commission (CRTC) Broadcasting Order 2009-340, issued June 11, 2009 and Broadcasting Order 2009-340-1, issued January 24, 2012, Pelmorex has established the National Alert Aggregation & Dissemination System (NAAD System), assisted by a Governance Council of public and private stakeholders." Pelmorex Alerting Services – National Alert Aggregation & Dissemination System This partnership is under the supervision of "The Pelmorex Alerting Governance Council. It includes representatives of the Senior Officials Responsible for Emergency Management, which has federal, provincial and territorial oversight for emergency management, as well as representatives from other federal government departments, Pelmorex, broadcasters, BDUs and the Canadian Association for Public Alerting and Notification." (Broadcasting Regulatory Policy CRTC 2014-444) Then the approach became mandatory in 2014 : Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014-447 and 2014-448 (see the cell below for the extract);

(continued)

	Following this decision, Public Safety Canada requests the Canadian Radio-Television and Telecommunication Commision (CRTC) Interconnection Steering Committee (CISC) to assist for the validation of the Wireless Public Alerting Service (WPAS) for Canada (Letter of Mission, CISC, 2014): "Mobile Phone and network integration specifications are required to enable the delivery of Cell Broadcast Alerts over Canadian Mobile Operators' LTE Networks using the Warning Message Delivery function within LTE" "The WPAS stakeholders include wireless carriers; federal, provincial and territorial alerting authorities; Pelmorex Communications, the owner of the NAAD system; wireless telecommunications equipment providers and vendors; and handset manufactures". It must take into account, from the start, the compatibility with the American Emergency Alerting System. The system was set up successfully in 2018. 2019: The CRTC approves the governments application to conduct provincial/territorial public awareness tests twice annually, during May Emergency Preparedness week, and the month of November. (Telecom Decision CRTC 2019-239)
Legislation on warning republishers and MNO	Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014-447 and 2014-448 "The Commission requires broadcasters to fully participate in Canada's National Public Alerting System. By 31 March 2015, broadcasters in Canada will be required to alert Canadians of imminent threats to life. Campus, community and Native radio and television broadcasters, as well as radiocommunication distribution undertakings, will be required to do so by 31 March 2016."
CAP reference	Yes. In the Public Safety Canada requests to the Canadian Radio-Television and Telecommunication Commission (CRTC) Interconnection Steering Committee (CISC) of 2014, PSC asks that the system must be based on the CAP-Canadian profile specification.
Note	Official Languages Act 1988 As such, the Wireless Public Alerting platform shall be architected to deliver bilingual alerts.

Chile

Governance	Chile is a centralized country. Decree no. 156 of March 2002 Plan Nacional de Protección Civil : introduces the First National Civil Protection Plan, based on national, regional, provincial and community level of Civil Protection Committee. During a Crisis, the Emergency Operations Committee is constituted in the Emergency Operations Center (COE). The National Emergency Office (ONEMI) of the Ministry of the Interior and Public Security qualifies the COE, with Regional Relay. ONEMI is the coordinator of all crisis management actors. It is responsible of launching warnings via the National Emergency Warning Center (CAT National).
Different alerting authorities for different hazard?	There are different agencies per risk who feeds the CAT of the ONEMI with real time information on the risks. (Means of Detection) See table below:

Threat	Official organism
Earthquakes	National Seismological Center of the Seismological Service of the University of Chile - Centro Sismológico Nacional (CSN) del Servicio Sismológico de la Universidad de Chile
Tsunamis	Hydrographic and Oceanographic Service of the Chilean Navy - Servicio Hi-drográfico y Oceanográfico de la Armada de Chile (SHOA) Member of the Pacific Tsunami Warning System
Abnormal surges	General Directorate of the Maritime Territory and Merchant Marine -Dirección General del Territorio Marítimo y de Marina mercante (DIRECTEMAR)
Volcanic eruptions	National Service of Geology and Mining - Servicio Nacional de Geología y Minería (SERNAGEOMIN)
Forest fires	National Forestry Corporation - Corporación Nacional Forestal (CONAF)
Threats of Hydrometeorological origin: Frontal Systems, Floods, Alluvions, etc.	Chilean Meteorological Office - Dirección Meteorológica de Chile (DMC), General Water Directorate - Dirección General de Aguas (DGA), National Geology and Mining Service - Servicio Nacional de Geología y Minería (SERNAGEOMIN), among others
Droughts	Directorate General of Water - Dirección General de Aguas (DGA), Meteorolo-gical Directorate of Chile - Dirección Meteorológica de Chile (DMC), among others.

Source: EENA Case study, Public Warning in Chile, Resilient Structure, 2018.

Different alerting authorities for different hazard? (*continued*)	In the specific case of Tsunami, the SHOA operates the National Tsunami Warning System (SNAM), as a member of the Pacific Tsunami Warning Center (PTWC – Hawaii; United States). The SNAM alerts the ONEMI and the Armed force of a confirmed tsunami risks. Then the ONEMI activates the network of sirens install on the coast with the message "Tsunami Alarm and Evacuation to Safe Area" via loudspeaker.
Who is in charge of establishing the Emergency Alerting System?	National Emergency Office (ONEMI), via the National Emergency Warning Center CAT. The Emergency Alert System in Chile is called SAE. "Unified Central Platform (PCU): This is the central platform, managed by ONEMI, which is part of the SAE and receives the warning signals emitted by the different means of Detection and then generates and controls the sending of georeferenced alert messages to the Dissemination Media." Decree No. 60, Reglamento para la Interoperación y Difusión de la Mensajería de Alerta, Declaración y Resguardo de la Infraestructura Crítica de Telecomunicaciones e Información sobre Fallas Significativas en los sistemas De Telecomunicaciones, of April 4, 2012. Ministry of Transport and Telecommunications, Chile.

(continued)

Legislation on warning republishers and MNOs	Decree No. 60, Reglamento para la Interoperación y Difusión de la Mensajería de Alerta, Declaración y Resguardo de la Infraestructura Crítica de Telecomunicaciones e Información sobre Fallas Significativas en los sistemas De Telecomunicaciones, of April 4, 2012. Ministry of Transport and Telecommunications, Chile. "Means of Dissemination: Corresponds to the different modalities or technical devices, whose primary purpose is to transmit the alert messages generated by the PCU, to the geographic areas specified in each message and defined by ONEMI, such as specific equipment and computer applications for the transmission of geo-referenced alert messages transmitted by mobile network cell broadcast services of mobile networks, over sound and radio broadcasting links, by internet services or by other means that can be technically intended for this purpose." Mobile Network Operators are only one of the channels of this decree. However, there is a full section (n° III) dedicated to "Interoperation between the Emergency Alert System and Operators" Article 10 Operators must ensure that their means of dissemination offers security conditions and reliability that allows them to comply with the obligation of transmission of alert messages. This decree 60 from 2012 mentions cell-broadcast technology on the 2G/3G networks.
Legislation on warning republishers and MNOs	Important point to notice: This decree 60 includes the obligation of the alert's receiver device to be in conformity with the alerting system: "Terminal devices receiving alert messages, such as radio, television, cell phone receivers and loudspeakers, must have the ability to interoperate and comply with technical specifications defined by the Undersecretariat for each case." The European Emergency Number Association EENA report of 2018 called "Public Warning in Chile; EENA Case Study Document" informs us that there is even an "SAE Homologation Room" whose role is to guarantee that the telecommunication of alert messages is operated correctly. "Since 2017, all mobile telephone terminals must have a technical verification seal that guarantees their compatibility with the SAE."
Mention of CAP in the legislation	There is no mention of CAP in the legislation of the Decree 60 from 2012. However, means of broadcast must comply with the specifications establish by ONEMI. CAP compatibility should not need a change in the legislation to ensure its implementation.

European Union

Governance	The European Union supranational political and economic union of 27 member states. It is founded mainly on the Treaty on European Union and the Treaty on the Functioning of the EU. Member States confer powers on the EU to attain objectives that they have in common. (EU-LEX-definition) The European Union gathers 27 Member States. Each of them is responsible for their own crisis management. However, the European Commission has established an EU Civil Protection Mechanism: "The Mechanism aims to strengthen cooperation between the EU countries and 9 participating states on civil protection to improve prevention, preparedness, and response to disasters. When an emergency overwhelms the response capabilities of a country in Europe and beyond, it can request assistance through the Mechanism. "(EU Civil Protection mechanism, 2023) The European union has the legislative power to establish Directives. They are legal acts that requires Member States to achieve particular goals without dictating how the Member States should achieve those goals.
Different alerting authorities for different hazard?	Yes. Each Member State can establish their own Alerting Strategy, with their own national specificities.
Who is in charge of establishing the Emergency Alerting System?	The European Directive 018/1972 establishing the European Electronic Communications Code (hereinafter EECC) includes an obligation for Member States to establish a Public Warning System in the article 110. Each country is in charge of establishing their own Alerting System, as a Directive does not impose "How" to establish it. However, Europe has settled the criteria that they must respect in terms of Alerting System – See next line for more description. To be noted: The European Union, based on the Member States political project, has launched years ago the satellite constellation called Galileo, to ensure globally a European Geo-positioning Service. In this service, some parts of the signal are booked for broadcasting an alert via Satellite when the Member States would need it. The Stellar project, due for 2024, is establishing demonstrations of this alerting prototype service, establishing the feasibility and utility of such new alerting channel. As the Galileo infrastructures are coordinated by European Institution, they are in charge of establishing this specific channel. The goal is to provide this service to the National Authorities of the Member States in complement of the existing National Public Warning Systems. To ensure the reach of this global service, European Union has taken a Regulation 2019/320 of 12 December 2018 in order to ensure caller location in emergency communications from mobile devices. It implies that each smartphone sold in Europe is compatible with the Galileo system.

(continued)

Legislation on warning republishers and MNOs	The article 110 (1) of the Directive (EU) 2018/1972 establishing the EECC sates that Member States shall ensure that, "public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned." MNOs are "Mobile number-based interpersonal communications services". It does not mention explicitly Cell-broadcast or Location-based SMS technologies, as European directives have no power to decide how the warning should be republished. So Member States may decide to go for an alternative channel such as an application. The Article 110(2) covers this case, stating that this is possible at the condition that is has an equivalent effectiveness "in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned" and is "easy for end-users to receive". The recital 294 EECC explains the word "easy" as : 'it should not require end-users to log in or register with the authorities or the application provider" Even if no European legislation on the Warning Republisher imposes a specific technology, the article 110(2) of the EECC Directive 2018/1972 states that the Body of European Regulators for Electronic Communications (BEREC) must issue Guidelines to assess the effectiveness of alternative Public Warning Systems using means of electronic communications services (BEREC 2019). Criteria are based on Coverage (geographical and in terms of population) and on the Capacity to Reach End-users (roamers, devices, languages, etc.)
CAP reference	Not at the European Level. A European Directive cannot impose a specific way to implement a Public Warning System, so there can't be mention of the CAP in the EECC directive. The BEREC guideline on the effectiveness of PWS does not mention it neither. To be noted: Belgium and Netherlands laws*, who have established a Public Warning System before this European Directive, do not mention CAP either. However, on both countries, the current Public Warning System is using CAP. - * Regulation of the Minister of Economic Affairs and Climate, 2023 laying down rules for providers of public mobile communication networks regarding the NL-Alert alert (Regulation alarm service NL-Alert 2023) - * Royal Decree on sending a short text message in case of imminent danger or major disaster, 23rd of February, 2018

United States of America

Governance	Federation of states. "Under all conditions the President and, except to the extent the public alert and warning system is in use by the President, Federal agencies and State, tribal, and local governments can alert and warn the civilian population in areas endangered by natural disasters, acts of terrorism, and other man-made disasters or threats to public safety;" Title V, National Emergency Management, sect. 526, IPAWS MODERNIZATION ACT OF 2015 IPAWS-OPEN is the FEMA national system for local alerting that provides authenticated emergency and life-saving information to the public through mobile phones using Wireless Emergency Alerts (WEA), to radio and television via the Emergency Alert System (EAS), and on the National Oceanic and Atmospheric Administration (NOAA) Weather Radio. The National Public Alert and Warning System (NPWS) ensures that the President can broadcast a national warning message in the most severe conditions.
Different alerting authorities for different hazard?	Yes. Each approved Alerting Authority can establish its own Alerting Strategy, with its own specificities. IPAWS-OPEN "is a federated system of systems that enables local Alerting Authorities to independently craft and transmit alerts targeted for their communities, using technology and protocols managed by IPAWS. These alerts, once verified through the IPAWS-OPEN platform, are distributed through private sector radio and television partners through the EAS and WEAs to cell phones and similar devices" [IPAWS strategy for 2022-2026] It consists of over 1700 Alerting Authority partners in 2022.
Who is in charge of establishing the Emergency Alerting System?	The Integrated Public Alert and Warning System (IPAWS) program was established under Executive Order (E.O) 13407 in 2006. IPAWS is FEMA national system: FEMA PUBLIC LAW 114–143—APR. 11, 2016 : "''Integrated Public Alert and Warning System Modernization Act of 2015'' : States that the Administrator should "implement the public alert and warning system to disseminate timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety."[…]" include in the public alert and warning system the capability to adapt the distribution and content of communications on the basis of geographic location, risks, and multiple communication systems and technologies, as appropriate and to the extent technically feasible;"[…] ''include in the public alert and warning system the capability to alert, warn, and provide equivalent information to individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency, to the extent technically feasible;" It establishes the Subcommittee of the National Advisory Council established under section 508 of the Homeland Security Act of 2002, in charge of the Integrated Public Alert and Warning System Performance supervision. This subcomittee is composed of several public representative, but also representatives of the "communication service provider" - MNOs

(continued)

Legislation on warning republishers and MNOs	WEA was established by the WARN Act. See Warning, Alert and Response Network (WARN) Act, Title VI of the Security and Accountability for Every Port Act of 2006, 120 Stat. 1884, codified at 47 U.S.C. § 1200, et seq. (2006) (WARN Act). WEA is developed together with FEMA and participating Commercial Mobile Service (CMS) providers based on standards created by the Alliance for Telecommunications Industry Solutions (ATIS), the Telecommunications Industry Association (TIA) (jointly, ATIS/TIA), and the 3rd Generation Partnership Project (3GPP). The last version WEA 3.0 contains an enhanced geo-targeting capability, released in November 2019. A "Participating CMS Provider" is a Commercial Mobile Service Provider that has voluntarily elected to transmit Alert Messages under Part 10 of the Commission rules. Please note that the Communications Security, Reliability, and Interoperability Council (CSRIC) IV, Working Group Two, Wireless Emergency Alerts, Geotargeting, Message Content and Character Limitation Subcommittee, Final Report at 7 (2014), mentioned that some small CMS Providers may not comply with the standards as they find the cost deployment of Cell-broadcast too prohibitive.
CAP reference	CAP is not mentioned in the Law explicitly, but the law recommends the adoption of international standards (which CAP one such standard). The CMSAAC (Commercial Mobile Service Alert Advisory Committee) recommends in the CSRIC report 2014 to follow the CAP standard for the message. In the 2022-2026 Strategic plan for IPWAS, it is written that "devices receive alerts from IPAWS in a standard message format called the Common Alerting Protocol".

Legislation cited

Australia

State Emergency and Rescue Management Act, 1989 (NSW) legislation.nsw.gov.au/view/pdf/asmade/act-1989-165

Emergency Management Act, 1986 (Vic) https://www.legislation.vic.gov.au/in-force/acts/emergency-management-act-1986/047

Disaster Management Act, 2003 (Qld) https://www.legislation.qld.gov.au/view/pdf/inforce/current/act-2003-091

Emergency Management Act, 2005 (WA) https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_36944.pdf/$FILE/Emergency%20Management%20Act%202005%20-%20%5B01-a0-03%5D.pdf?OpenElement

Emergency Management Act 2004, (SA) https://www.legislation.sa.gov.au/__legislation/lz/c/a/emergency%20management%20act%202004/current/2004.30.auth.pdf

Emergency Management Act, 2006 (Tas) https://www.legislation.tas.gov.au/view/pdf/authorised/2020-05-06%202020-06-01/act-2006-012

Emergencies Act, 2004 (ACT) https://www.legislation.act.gov.au/a/2004-28

Northern Territory Disasters Act, 1979 https://legislation.nt.gov.au/en/Bills/Northern-Territory-Disasters-Bill-1979-S-367?format=assented

RCN.900.116.0023 – Commonwealth Attorney-General Department, 'Australia's Emergency Warning Arrangements' (April 2013). https://naturaldisaster.royalcommission.gov.au/publications/exhibit-31-023001-rcn9001160023-australias-emergency-warning-arrangements

HAF.9002.0001.0020 ROYAL COMMISSION INTO NATIONAL NATURAL DISASTER ARRANGEMENTS; "RESPONSE OF DEPARTMENT OF HOME AFFAIRS TO NOTICE TO GIVE INFORMATION DATED 1 MAY 2020 (NTG-HB2-244)" https://naturaldisaster.royalcommission.gov.au/publications/exhibit-30-027002-haf900200010002-response-notice-give-information-ntg-hb2-244

Broadcasting Services Act (Cth), 1992 https://www.legislation.gov.au/Details/C2017C00201

Code of Practice for Warning Republishers, 2013 https://knowledge.aidr.org.au/media/5657/warning-republishers-code-practice.pdf

Canada

Emergency Management Act, 2007 https://laws-lois.justice.gc.ca/eng/acts/e-4.56/page-1.html

CRTC Chronology of Public National Alerting in Canda https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sstm-chr-en.aspx

Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014-447 and 2014-448 https://crtc.gc.ca/eng/archive/2014/2014-444.pdf

Radiocommunication Act, 1985 https://laws-lois.justice.gc.ca/eng/acts/r-2/

Telecommunications Act, 1993 https://laws-lois.justice.gc.ca/eng/acts/t-3.4/FullText.html

Broadcasting Act, 1991 https://laws-lois.justice.gc.ca/eng/acts/B-9.01/

Letter of Mission, CISC, 2014: available from ITU on demand, summary available within the Broadcasting Regulatory Policy CRTC 2014-444 quoted above

Telecom Decision CRTC 2019-239 https://crtc.gc.ca/fra/archive/2019/2019-239.pdf

Official Languages Act, 1988 https://laws-lois.justice.gc.ca/PDF/O-3.01.pdf

Chile

Decree no. 156, Plan Nacional de Protección Civil, March 2002 https://www.bcn.cl/leychile/navegar?idNorma=199115&idParte=

EENA Case study, Public Warning in Chile, Resilient Structure, 2018 eena.org/knowledge-hub/documents/public-warning-in-chile-resilient-culture/

Decree No. 60, Reglamento para la Interoperación y Difusión de la Mensajería de Alerta, Declaración y Resguardo de la Infraestructura Crítica de Telecomunicaciones e Información sobre Fallas Significativas en los sistemas De Telecomunicaciones, 4 April 2012 https://www.bcn.cl/leychile/navegar?idNorma=1039988&idParte=

Europe

EU-LEX definition https://eur-lex.europa.eu/EN/legal-content/glossary/european-union.html

EU Civil Protection Mechanism, 2023 https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

European Directive 2018/1972 establishing the European Electronic Communications Code https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1972

Regulation 2019/320, 12 December 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A055%3ATOC&uri=uriserv%3AOJ.L_.2019.055.01.0001.01.ENG#:~:text=Commission%20Delegated%20Regulation%20%28EU%29%202019%2F320%20of%2012%20December,caller%20location%20in%20emergency%20communications%20from%20mobile%20devices

Regulation alarm service NL-Alert, 2023 https://wetten.overheid.nl/BWBR0047721/2023-01-01

Royal Decree on sending a short text message in case of imminent danger or major disaster, 23 February 2018 https://centredecrise.be/fr/documentation/legislations/23022018-arrete-royal-relatif-lenvoi-dun-message-texte-court-en-cas-de

USA

IPAWS MODERNIZATION ACT, 2015 https://www.congress.gov/congressional-report/114th-congress/senate-report/73/1

IPAWS strategy for 2022-2026 https://www.fema.gov/sites/default/files/documents/fema_ipaws-strategic-plan-fy-2022-2026.pdf

Executive Order (E.O.) 13407, 2006 https://www.federalregister.gov/documents/2006/06/28/06-5829/public-alert-and-warning-system

Homeland Security Act, 2002 https://www.dhs.gov/homeland-security-act-2002

Warning, Alert and Response Network (WARN) Act, 2006 https://www.congress.gov/bill/109th-congress/house-bill/5785/text

Communications Security, Reliability, and Interoperability Council (CSRIC) IV, Working Group Two, Wireless Emergency Alerts, Geotargeting, Message Content and Character Limitation Subcommittee, Final Report 2014 https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_CMAS_Geo-Target_Msg_Content_Msg_Len_Rpt_Final.pdf

Other countries

- **Philippines**: Republic Act No. 10639 "Act mandating the telecommunications service providers to send free mobile alerts in the event of natural and man-made disasters and calamities", June 2014 https://www.officialgazette.gov.ph/2014/06/20/republic-act-no-10639/
- **Indonesia**
    - Law No. 24/2007 https://leap.unep.org/countries/id/national-legislation/law-republic-indonesia-no-242007-concerning-disaster-management#:~:text=The%20Law%20establishes%20a%20National,determines%20what%20constitutes%20a%20disaster.
    - CABARET report on Indonesia, 2018 https://cabaret.buildresilience.org/images/NPP-Indonesia.compressed.pdf
    - Regulation 93/2019 https://peraturan.bpk.go.id/Home/Details/129198/perpres-no-93-tahun-2019#:~:text=PERPRES%20No.%2093%20Tahun%202019,Dini%20Tsunami%20%5BJDIH%20BPK%20RI%5D
    - UNDRR, "Limitations and challenges of early warning systems: A case study of the 2018 Palu-Donggala Tsunami" https://www.undrr.org/publication/limitations-and-challenges-early-warning-systems-case-study-2018-palu-donggala-tsunami

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

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

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

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

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

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

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

Africa

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

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

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

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

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route 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: ituteguciglapa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

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

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

Asia-Pacific

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

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

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

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

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

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

Email: itu-ro-southasia@itu.int

CIS

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

Europe

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

Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

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

ISBN: 978-92-61-38191-2

9 789261 381912

Published in Switzerland
Geneva, 2023