Review

International Journal of
Distributed
Sensor Networks

International Journal of Distributed Sensor Networks
2019, Vol. 15(2)

DOI: 10.1177/1550147719829960
journals.sagepub.com/home/dsn
SAGE

Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service

Zayan EL Khaled and Hamid Mcheick

Abstract

The failure of communications systems may cause catastrophic damage to human life and economic activities as people are unable to communicate with each other in a timely manner and with a convenient quality of service. Therefore, the exchange of information is more than necessary for people in their everyday life or during harsh environments to prevent the death and injury of thousands of individuals. The study of communications systems behavior in harsh environments helps to design or select more resilient technologies that are capable of operating in challenging conditions. This article reviews existing approaches, major causes of failure, and weaknesses of communications systems during extreme events. First, we highlight the importance of communications systems, and then we examine related works, how communication may fail, and the effect of this failure on human life in general and during extreme events response. Furthermore, we study and analyze how communications are used during various stages of extreme events, and we identify the main weaknesses and limitations that communications systems may suffer based on many case studies. To conclude, we identify and discuss relevant attributes, requirements, and recommendations for communications systems to perform with a suitable quality of service during harsh environments and to reduce risks of communication failure in challenging conditions.

Keywords

Communications system, communications network, extreme events, disaster, communications failure, emergency network, telecommunications, QoS improvement, harsh environment

Date received: 15 August 2018; accepted: 21 December 2018

Handling Editor: Shinsuke Hara

Introduction

Calamities, defined as generally unplanned events that cause significant losses, have become a common occurrence, consistently taking the lives of thousands of people. Extreme events in many parts of the world have caused serious damage to goods and led to significant trauma for affected people and their loved ones. Natural disasters (ND) cause serious deterioration of social and economic activities, ranging from habitation to nutrition, health facilities, communications systems (CS), power supply, and transportation. During harsh environments (HE), the provision of direct and indirect support for human needs is a substantial challenge.[1]

Department of Computer Science, University of Quebec at Chicoutimi, Chicoutimi, QC, Canada

Corresponding author:
Zayan EL Khaled, Department of Computer Science, University of Quebec at Chicoutimi, Chicoutimi, QC G7H 2B1 Canada.
Email: zayan.el-khaled1@uqac.ca

It is difficult for people to deal with hard circumstances that take place during natural or man-made disasters. Disaster management encompasses several operations such as immediate response, recovery, mitigation, and preparedness for decreasing the effect of future calamities. Rescuers require fast and efficient access to information for effective disaster management (DM) processes. Extreme events may hit a wide area, and therefore, many organizations may be involved in rescue operations, involving government and voluntary organizations working together as a single team to help the injured, save lives, and protect facilities.[2]

HE create significant immediate challenges for authorities in many fields. Indirect damages are also set in motion by a catastrophe, such as social problems, economic pressures, loss of tourism, a drop in industry, and so on.[3] As extreme events increase in frequency, they strike different countries in various ways: developing nations suffer from high quantities of victims and hard economic losses, while developed countries are able to reduce losses due to their use of best practices and efficient infrastructure.[4]

In such circumstances, the most important goals are saving lives, goods, and all necessary infrastructure for extreme events mitigation as quickly as possible. Doing so may allow for quicker rescues and reduce the impact of anxiety on victims.[1] During the first 72 h after a ND,[5] rescuers are more likely to save lives of victims, and fast evaluation of losses is required. CSs are essential during this period to support the exchange of information between entities such as humanitarian organizations, communities, and governments.

Importance of communication systems in HE context

Technology is so integrated into everyday life for the majority of people that the development of a society or country is proportional to its progress in information technology (IT).[6] Recently, communication technology (CT) has evolved dramatically and CSs have become essential, not only for basic communication but also to have access to media, services, and data supplied by companies, organizations, government, and so on.[7]

The role of telecommunications infrastructure (TI) is not only limited to people's daily routine as described earlier. During HE, they also provide a way for people to declare their safety or verify the safety of their relatives through emergency calls and priority phone lines. They also afford essential communications services in order to keep critical government services such as police and health care running. In extreme events, CSs provide fundamental response and recovery activities as they help connect victims to relatives, rescuers, and relief organizations in the aftermath of extreme events or crises.[8]

Reliable and accessible CSs are also important to a community's resilience as they afford important options for people, government, and relief organizations to deal with risks during HE. Immediately preceding catastrophe, telecommunications are used to broadcast warning information about what is happening. Then, people are able to take action in order to prevent or reduce the effect of these calamities. Therefore, it is obvious that CSs play a critical role in disaster warning, management, and alleviation. During ND like earthquakes, hurricanes, and tsunamis, traditional means of communications such as fixed or wireless phones might be damaged.[9] Thus, each country must prepare alternatives for such situations so that DM organizations can respond quickly and efficiently. Thus, DM teams must be skilled and provided with the latest CSs to assess losses and damages, and coordinate their operations in the affected areas.

ND such as the earthquake in Haiti and the tsunami in Japan or attacks like the September 11 terrorist attack in New York have demonstrated the importance of CSs in preventing losses and coordinating relief actions. In the aftermath of crisis, responder teams such as volunteers, firefighters, security staff, and health care personnel are sent quickly to the damaged zone. Robust CSs must always be ready to use, especially during the early response time after a crisis as they are essential to saving lives.

Rapid technological advances allow for greater efficiency in dealing with the effects of crises by reducing impact on human life as well as social and economic activities, protecting and supporting facilities, and getting medical help to the injured. Each stage of DM (preparedness, response, mitigation, and restoration) requires its own technological solutions.[1] Many areas such as space technology, modern CS, health care and diagnostics, artificial intelligence, green energy, and remote-controlled robots are useful in DM operations for rescue and relief efforts.

Communication breakdown effect

The failure of CS is widely known to occur in almost all extreme conditions. The breakdown of TI, whether complete or partial, causes inefficiency and delays in emergency relief efforts and response, which leads to loss of life and preventable injuries.[10] Due to increasing dependence upon CS during extreme events, the risk of communication failure is high, despite increasing immunity and protection of these means against disasters, HE and calamities. An extreme event situation with a severely disrupted TI amplifies chaos and uncertainty.

Poor communications between responders can severely hamper assessment and relief efforts, and prevent affected populations from connecting with responders and relatives.[5]

During DM actions, information and instructions may be transferred through a long series of organizations, before arriving at the right destination. As an example, pictures, real-time video, and other pertinent inputs related to the damaged areas are sent from rescuers to their management offices and other remote command centers. Similarly, relevant data and instructions are sent from headquarters to command centers and then to rescuers.[2] Effective DM necessitates robust CS to provide a continuous exchange of information between rescuers and remote command centers. Any failure or disconnection of this can generate disorder of disaster response operations.

Furthermore, the damaged area may become isolated by the total or partial failure of CS. In this case, the ability to send reports, information, or data to the outside world or remote headquarters will be reduced. For example, during a tsunami, we need to send information related to the disaster everywhere, even to unaffected areas, in order to broadcast early warnings and ensure evacuation from crisis zones. Moreover, we risk losing time during the 72 golden hours immediately following a disaster, the time period when we are most likely to save lives.[3] By using efficient CS, we are able to send first response teams quickly to rescue the population of the affected area.

Communication failure may occur in the majority of extreme event scenarios which provoke loss of lives and properties.[11] Also, the damage to CS along with the increase in traffic crossing the network disrupts relief operations. Thus, rescuers are not able to exchange information and people cannot communicate their position or ask for assistance, and the entire relief operation is hardly managed.[12] Besides physical damage, the remaining CSs are inadequate to handle the increased need to make calls as the network becomes overloaded by the huge number of communication attempt.[13]

Coping with crisis

Over the last few years, calamities have caused, even in developed countries, extreme events that may easily collapse CS.[10] In such contexts, the needs of rescuers and the affected population are directly proportional to the amount of diversity and elaboration of the network infrastructure, as it increases dependence on these systems along with the risk of failure and losses. However, modern CSs can equally supply efficient and effective ways to help governments to deal with challenging conditions, and quickly reestablish affected economic and social life. Over the past few years, the evolution of CS has led to the development of innumerable services and applications based on the Internet such as video streaming and sharing, cloud services, social media, and so on. Social media applications are a particularly good example, as they were useful for checking the safety of people in the aftermath of a disaster when CSs were destroyed or overloaded and it was hard to communicate by phone or text messages. In addition, these applications were highly efficient as users are able to make posts online to propagate and obtain information about the crisis.[7]

Yet the application of technologies during HE has revealed serious inefficiencies that have challenged cooperation between rescue teams. For example, in 2004, after Hurricane Katrina, communication tools were seriously damaged, resulting in serious challenges for victims and first response teams.[14] In addition, a few minutes after the explosion of a fireworks depot in the Netherlands in 2000, which destroyed a significant proportion of a city, the GSM (Global System for Mobile communications) network overloaded and went out of service.[3] Many other examples prove that current CSs have various weaknesses and limitations that may hamper and challenge emergency response. Important weaknesses are physical destruction, lack of compatibility between technologies, and the congestion of CS.

Furthermore, restoring connectivity, even temporarily among rescue teams, is a critical goal for helping rescuers to report their inputs and synchronize their actions.[13] Because quick repair of CS during golden hours may boost operations, there is a need to install flexible infrastructure that is able to restore connectivity immediately. The advanced technology used for DM may support relief organizations and provide necessary feedback for any action to take during catastrophes.

In addition, CT was integrated into the DM process a long time ago, as efficient CSs are important to a community's resilience.[9] Furthermore, the use of CT is essential during the four phases of DM: preparedness, mitigation, response, and recovery. Also, information and communications technologies (ICT), which have had significant progress recently, help to integrate many CSs together. Hence, the use of CT in DM is also growing.

Challenges restoring communication

There are serious challenges during the deployment of CSs under extreme conditions.[13] First, the system must operate without knowing any previous information about its environment; thus, the installation and configuration must be done on the fly and as quickly as possible in order to restore, strengthen, or substitute the failed part of the infrastructure. Second, CSs must be scalable, resilient, and energy efficient to deal easily with unknown conditions and limited battery life of many devices; thus, CSs have to be installed on demand in full conformity with current needs and required location. Third, as many entities are concerned in the rescue operations, CSs should interoperate with heterogeneous technologies; the goal is to support various standards and devices, so that all responders will be able to communicate together, coordinate operations, and receive requests from affected populations. There are many other challenges that we will examine in detail in this article such as reliability and robustness to support critical requirements, flexibility to self-organize when architecture changes in order to minimize delays, and facilitating the deployment of components without needing existing TI.

Research objectives

Despite the benefits of modern CS to society, failures of TI present serious consequences and risks due to increasing dependence upon these instruments. This article addresses weaknesses and limitations of CS that can cause ineffective performance, low communication quality of service (QoS), or even dysfunction during extreme contexts. To begin, we examine the impact of the utilization of CT during HE, in addition to causes of communications failure. Then, a special focus is given to the relationship between recent extreme events and telecommunications in order to review previous failures and successes and identify the attributes and characteristics that CS should have to improve performance and QoS of communications during HE contexts.

The remaining portion of the article is arranged as follows. In section 2, a review of the literature is presented. In section 3, telecommunications usage during extreme conditions is examined. In section 4, case studies of the utilization of CS during several challenging contexts are presented. In section 5, we discuss and identify recommendations based on the previous section. In section 6, attributes that modern CSs should have are introduced based on many case studies and previous examples. We finish this article by the conclusion and next steps.

Related works

The importance of communications during disasters has been a major area of study over recent years with a number of research papers published highlighting the need for reliable means of communication in all DM stages. In this section, we depict related work and pinpoint the contribution of this article. Ferris and Petz[15] review the major ND that have hit various regions of the world and discuss their effects on society. Another one[16] examines, in detail, a design process for CS to be disaster tolerant and gives best performances during the crisis. Rautela and Pande[17] highlighted the problems and issues that can occur if people are not well prepared for DM. The Guidebook[1] provides assistance for governments, professionals, and volunteers to find convenient solutions for many difficulties occurring during ND. Townsend and Moss[10] have detailed the need for CS during the disaster recovery process.

Schryen and Wex[18] examined solutions for risk evaluation and mitigation provided by information systems research in ND management. Brown and Mickelson[19] discussed a framework to investigate appropriate ICT to use in limited resource areas, mostly rural areas. Fragkiadakis et al.[20] have proposed a scalable network platform that provides a common architecture for interoperable and heterogeneous networks during catastrophes. Miranda et al.[13] surveyed possible alternatives for critical communications by deploying a network without any previous information about the communications environment. Gomes et al.[21] did a survey of wide regional failures and solutions for achieving resilient routing, including disaster-aware routing. Saim et al.[12] examined the utility of cognitive radio technologies for emergency communications response and confirm that they are very convenient to fulfill the hard requirements of these systems.

Bartolacci et al.[22] described parameters to conveniently choose the location of mobile network base stations and other communications equipment in an affected area. The article[11] sets out the architecture for solving the problem of filtering or prioritizing for limited bandwidth of Mobile Ad Hoc Networks. Wang et al.[23] discussed how smartphone systems work effectively in a disaster through the use of embedded sensors and emergency applications.

Srinivasarao et al.[24] completed a survey of emergency CS architectures including warning processing and transmission network architectures. Premkumar and Jain[14] examined some specifications to improve the efficiency of a CS during relief operations in the aftermath of a disaster. Leah Davis and Robbin[25] examined some causes of communication failure during the response to Hurricane Katrina. They also studied how failures of communication, management, and information sharing reduce network organizational effectiveness. In survey, Wang et al.[23] depicted and displayed communication system architectures, research challenges, and performance specifications for intelligent power system management. Markakis et al.,[26] examined many new challenges that emergency service providers will encounter with the arrival of 5G. Dial et al.[27] were charged with evaluating current systems and found areas of opportunity for improvement for Fujian Province's emergency systems. Channa and Ahmed[2] surveyed proposed frameworks for emergency communications response and possible security requirements to provide a secure and efficient exchange of information. Li[28] identified several challenges to deploy the emergency warning CS.

Discussion

As modern life is completely dependent on CT, the population can be more vulnerable when communication fails. Thus, the importance of communications has been a major area of study over recent years with a number of research papers published highlighting the need for reliable means of communication during extreme events contexts or daily activities. Their principle aim is to help provide people with their basic needs and activities, in addition to communicate with rescue teams and their relatives. According to our survey, most of the papers focus on specific technology or specific issues in CT, or how to adapt CS according to a particular context. During extreme events, many aspects are concerned in the use of CT for mitigation and response efforts, such as technical, social, procedural, and organizational. It was difficult to find a publication that dealt with all of these aspects by reviewing many disasters in order to find weaknesses and limitations to address the decrease of communications' QoS during HE.

Paper contributions

According to our knowledge, there is no detailed study that takes into account the usage of CS during many types of extreme events at the same time. Existing research papers have examined a single case in detail, or they focused on characterizing and dealing with a special context that may occur during HE. Our objective is to illustrate approaches, weaknesses, and limitations that may take place while using CS during extreme events in general in order to address the decrease of communications' QoS and propose resilient solutions for CS during HE. Our goal to provide reliable solutions for CS was based on the following idea: if a CS is reliable and efficient during challenging environments it will probably perform even better during normal conditions. To validate our findings, we studied many extreme events based on various criteria such as man-made or natural; whether affected countries were developing or developed; type of event, such as earthquake or tsunami; affected areas are rural or urban; and continents like Asia or America; and we considered temporal distribution in order to cover the digital era revolution up to current days. Then, we extracted the characteristics that such systems must have in order to provide a convenient and resilient communication QoS. These characteristics have been deduced according to a deep literature study of many papers that had examined recent extreme events to identify the technological weaknesses to be overcome. We will try to address some of these weaknesses through future research for reliable CS by comparing all common modern CT without prior judgment of which one is best suited. In brief, this article provides the following main contributions:

- Examine technologies and approaches taken to deal with CS failures during several extreme events.
- Illustrate standards, actions, and recommendations proposed by specialists and commissions to strengthen the resilience of CS.
- Provide an analytical global study of CS weaknesses and limitations based on a deep analysis of many extreme events contexts.
- Identify relevant attributes and requirements that CS should have to ensure a good communication QoS by taking into account many case studies in addition to practical, technical, contextual, social, and procedural realities. Best-suited CT will be selected through future research by using these attributes.

Disasters and telecommunications

The impact of natural extreme events

Natural or man-made disasters are frequently occurring, especially in recent decades as we can see in Figure 1. They also bring serious human losses of many tens of millions of victims, see Figure 2; equally economic losses exceeded hundreds of billions of dollars, see Figure 3. As an example, the earthquake of Haiti alone claimed 230,000 people's lives in 2010.[30] Although, in the aftermath of a disaster, the affected zone is in chaos. Let us take the earthquake that has hit Japan in 2011 as an example. It had 9.0 magnitudes, followed by a tsunami of 23 m high and accompanied by a nuclear crisis; as a consequence, already well-trained emergency response specialists and the world were dazed. By synthesizing consequences of many large-scale disasters, we obtain following conclusions:[5,7,25,30–33]

- The collapse of buildings and infrastructures: Besides the high human cost of extreme events that exceeded hundred millions of people, Figure 2, they additionally made many people homeless and waiting for help. Also, damages to economic activities and infrastructures' destruction caused the raise of total economic losses of many hundred billions of dollars in recent years, Figure 3.
- Paralysis of traffic in the damaged zone: Even remaining circuits were congested due to huge disaster response or evacuation of vehicles. Thus, external aid like disaster response workers and goods transportation is difficult to flow in damaged areas.[34] Also, airports may be

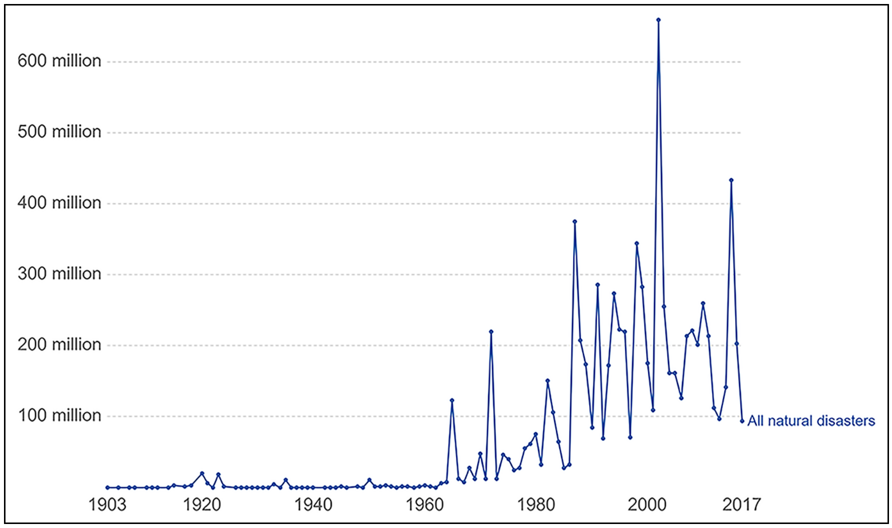

Figure 1. The number of global reported ND events. This includes those from drought, floods, biological epidemics, extreme weather, extreme temperature, landslides, dry mass movements, wildfires, volcanic activity, and earthquakes.[29]

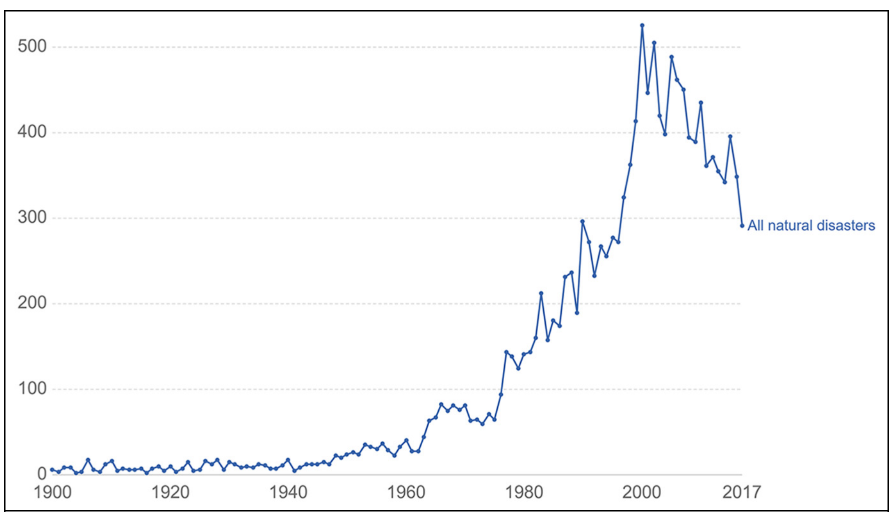

Figure 2. Global total number of people affected by ND. This is defined as the sum of the people who were injured, affected, and left homeless after a disaster.[29]

damaged, and as no plane could land, external aid could not be provided immediately during the golden 72 h. However, we still able to use helicopters to transport some limited resources, but the difficulty level of disaster response is still complicated.

- Paralysis of entire CS: The remaining networks could not be used due to traffic congestion or power outages. Then, the information about damages and needs in the damaged areas can hardly be accessed. Thus, without a clear understanding, it is difficult to allocate available resources efficiently and appropriately. Hence, the misplacement of disaster relief goods makes it impossible for victims, and human cost rise.
- Lack of professional disaster response workers: Their number is poorly sufficient, especially at the beginning of disasters when numerous local voluntary workers are to get involved in disaster response.
- Dysfunctional administrative command system: Every level of this system may be paralyzed, and

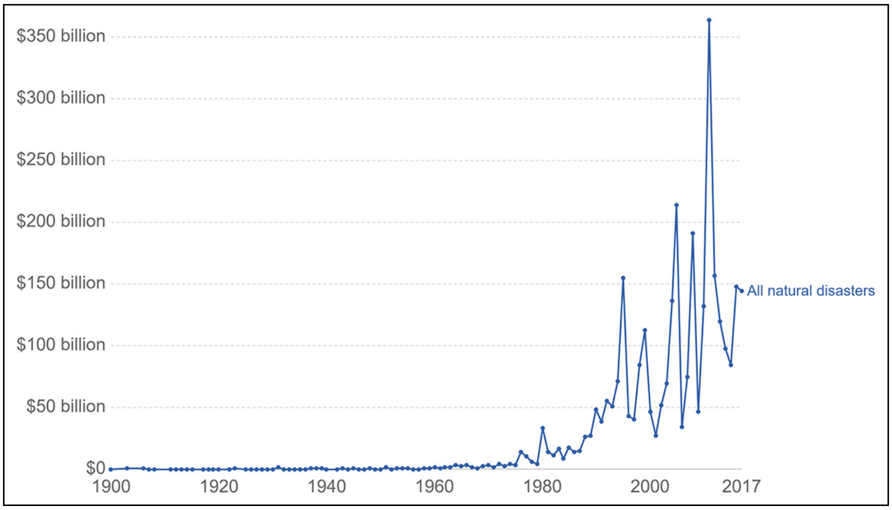

Figure 3. Total economic cost of damages as a result of global ND in any given year, measured in current US$, includes those from drought, floods, biological epidemics, extreme weather, extreme temperature, landslides, dry mass movements, extraterrestrial impacts, wildfires, volcanic activity, and earthquakes.[29]

the remaining system may be prevented from assuming the greatest responsibility of disaster response planning and administration.

- Bad coordination: The efficiency of rescue activities was low because there were no common communications tools between the workers. Also, poor communication causes interference with emergency response actions. Hence, emergency response operations were slow and many loosed lives could have been saved.

Losses and consequences due to telecommunication failure

Over the last decade, 3852 ND have killed 780,000, affected 2000 million people, and cost at least US$960,000 million.[4] ICTs are unavoidable in the prediction, detection, monitoring, and warning of the occurrence of ND. They also have a critical role during disasters' responses by providing efficient information exchange for entities concerned in recovery and rescue actions. Thus, emergency CSs are essential to all DM phases, namely, detection and prediction, warning, and relief operations.

To illustrate the importance of CS, during an earthquake in 2010,[5] when fuel was in short supply, the available stock was distributed only to local emergency services. The local operator was, therefore, not able to replenish its emergency generator fuel and many sites stopped functioning. Because telecommunications were not considered as an essential service, critical CSs were disrupted and the coordination of relief efforts was severely hampered.

Consequences of CS failure prevent efficient response in the aftermath of a disaster. Also, rescuers are more concerned to prevent any additional life losses, than reduce damage to properties and infrastructures. Relief operations may be severely delayed or paralyzed if the responding organizations are unable to communicate with each other and effective coordination becomes more complicated. In such time-sensitive situations, the loss of few minutes may reduce the gap between death and life for people in need for rescue.[35] Even if rumor is not risky in the same way as a delay in response efforts, however, it is able to establish a seriously confused environment. With the imbalance of communication channels, conflicting information about damages can spread panic and rumors at a situation when planned acts are necessary for efficient and quick relief.

In the literature, we can find many examples of loses due to communication failure such as the survey in Cole and Hawker.[36] It was reported also that during the northwest wildfire, first responders were not informed that the wind had shifted and the fire turned toward them.[37] The main challenges include the loss of communication and the lack of compatibility between CSs. The incapacity of emergency organizations to coordinate and communicate may cause catastrophic consequences on human life and properties as was mentioned in the fire of Okanogan Complex in August 2015.[38] To demonstrate these necessities, just examine the terrorist attacks of the World Trade Center (WTC), where 121 firefighters died due to the missing radio interoperability between police's radios and their devices.[37] The Virginia Tech shootings and the Katrina hurricane also proved the necessity of CS interoperability and collaboration between implied agencies.[39] In addition, in Sri Lanka, the tsunami caused the death of over 34,000 people due to the lack of an early warning system; there was sufficient time to evacuate coastal population if information about the coming disaster was available.[40] While in the case of extreme events, physical damage is unavoidable, in many other cases, the human death could be avoided if convenient measures and precautions had been taken. As in the case of Indian Ocean tsunami in December 2004, it provoked losses of over a quarter of a million deaths.[40]

How CS fails during disasters

During disasters, TI may fail through a variety of reasons. Many investigations demonstrate the main three reasons for CS failure:[41,42]

- Destruction of CS components
- Damage of supporting infrastructure
- Congestion

Each of these three reasons will be examined in detail in the next sections.

Physical destruction of network infrastructure. CSs are crucial to disaster response, but during the crisis, they could be easily paralyzed. The principal reason for communication failures may be physical damage of CS. Hurricane, flood, and earthquakes can all create significant damage to towns and their vulnerable communications components.[35] Physical damage can be also extremely expensive and time-consuming to restore as it may require maintenance or replacement of complex hardware, particularly if essential components such as cell towers or cables are concerned.

The weakness of telecommunication networks (TN) is due to the lack of a high degree of redundancy.[10] For example, fixed phone network architecture is conceived in a way that the simple loss of a fraction can instantly disconnect all neighborhoods. The New York 2001 attacks damaged a major routing center, isolating large parts of lower Manhattan from the telephone network. Yet, new "packet switched" technologies, such as the Internet, are more resilient to physical destruction, thanks to increased redundancy and advanced routing techniques to bypass destructed parts. Such networks can support serious damage before certain parts become out of service. However, in spite of its resilience, the Internet still vulnerable because it is installed through the old and nonredundant telephone and cable television networks copper wire in many parts of the world. Also, cable damage can be harder to repair as it is hidden underground; hence it may take a huge time just to locate the exact location of the damage.[41]

Although, wireless networks are highly variable in their vulnerability to physical node destruction and resulting loss of service.[10] For example, if a cell tower is severely damaged, in addition to the major service disconnection in its area, it will remain a serious problem as it is hard and costly to replace. Wireless links are also likely to be disturbed or damaged, as signals of different wavelengths can be extenuated by snow, heavy rain, or fog. Also, the transmitter itself can also be damaged or misaligned with its receiver.[35] Broadcasting services are extremely vulnerable as they are generally centralized at the metropolitan level. For example, the destruction of the WTC, which was the location of many TV and radio stations, has disconnected the broadcast services of many media stations. New architectures of wireless networks are more and more decentralized; the cell phone network is centralized at little scale in larger cities. Hence, the destruction of the base station may disturb service only in a small zone.

Like the majority of urban infrastructures, TN may be damaged in nearly all important disasters. Yet, it is not the scale of the disaster, but how the location of damages may coincide with the old and new communication facilities that are the determining factor. Although these problems may be less costly and less difficult to correct, they can be a serious challenge to relief efforts if they remain during the first 72 h of a disaster.[35]

Disruption in supporting infrastructure. Breakdowns caused by supporting infrastructure tend to be much more prevalent and detrimental to response and recovery efforts, even if they are less common than outages caused by physical damage. The electrical distribution network is the major supporting infrastructure for CS because electrical energy is needed for the operation of the majority of modern communication devices. Thus, power outages and insufficient fuel for power generators are the main reason for stopping CS.[30] For example, during the power outage of 2003 in the northeastern United States, mobile phone services failed as most antenna sites were powered by only 4–6 h of battery backup.

In addition, after an Earthquake on 2010, a local operator reported that only 16% of base stations in the affected region were rendered inoperable. However, just 28 h later, about 86% of base stations became inoperable and the cause was a power failure. In addition, after the Japan tsunami in March 2011, approximately 8000 mobile base stations were immediately disabled. Within 24 h, this number almost doubled when backup power systems became exhausted. These power outages were responsible for 85% of mobile communication breakdown during that time.[5]

While power systems are the major supporting infrastructure for CS installations, cooling systems are also critical and may fail independently of the power supply.[10] Finally, transport failures can also affect the fuel supply for backup generators. On September 11 New York attacks, the main communication device for a service provider was put offline due to a power failure and bad diesel fuel supply at the same time.

Disruption due to congestion. Even if physical components subsist after a disaster, CS can disrupt due to congestion. The consequence is temporarily the same as the failure is by physical damage. To understand the effects of congestion, just think about the road traffic if all vehicles are put together at the same time; surely, they will not be able to move. Abrupt peaks of traffic in circuit-switched networks, such as landline phones, may block the communication, but it can be restored relatively rapidly. However, in a packet-switched network, the consequence is simply performance degradation. As for SMS (short message service), the message will always be sent but will be late depending on the scale of the congestion.[43]

However, failures caused by congestion will progressively disappear as users change their communication behavior. In the meantime, congestion restricts voice traffic by 70%–95%, although packet traffic is only limited by 0%–30%.[44] In New York in 2001, both fixed and mobile communications experienced significant overload. Mobile phone networks recorded a 92% blocking rate, with call volumes increasing 10-fold.[4] In addition, the congestion caused by the peak of calls to verify the safety of people has induced a call restriction of 80%–90%.

CS in disaster recovery

This section highlights the role of CS in all phases of disaster recovery. These phases are organized as follows:[4,5,10,24,45,46]

- Disaster warning
- Emergency response
- Restoration and repair
- Reconstruction
- Redevelopment

We will try to understand the role and potential failures[42] of TI on each phase.

Disaster warning. Before a disaster, the principal mission of emergency communications is disaster notification.[24] Efficient warning and appropriate evacuation process allow individuals and communities to react accordingly to a threat and decrease the risk of injury, death, and goods damage. Communities need multiple channels of communication to ensure the reception of alert information, and the dissemination of knowledge and awareness. They are no single system that can be used in all situations; an efficient warning system should employ many channels of information and should be in a state of permanent readiness. Two types of communication methods are available for alerting:[46]

Mass methods: sirens, conventional radio, television, and so on.
Addressable methods: cellular mobile, telephone, Short Message Service, fax, paging, and so on.

The warning procedure can be detailed as follows: at first, sensors monitor their environment and send periodic information to a data center. The transmission may be done by wire lines, satellite, or wireless communications. In this center, received data are analyzed and processed; humans monitor the result 24 h a day to make a decision to issue or not a disaster warning. If a warning is to be issued, then the information is distributed to individuals in the disaster area by all possible means. Finally, technical efforts involve how warnings can be effectively distributed across the existing communication infrastructure with slight modifications to existing systems, without the need for human intervention.[24]

CS during emergency response. Emergency response activities begin nearly once a disaster has started. This period is characterized by doing immediate relief activities such as injured rescue and evacuation. During an emergency, official public safety systems are the most important CS.[10] Those systems supply first responders with the possibility to assess damages and coordinate their operations efficiently. Although they are prone to failure, these networks can supply basic voice services to support communications during an emergency.

In wide-scale disasters involving the response of several agencies, civil networks have become an essential means of emergency communication. This is due to the incompatibility of equipment used by response organizations, impeding interagency communication between stakeholders.[24] Also, civil networks offer greater data communication capabilities than their counterparts in public security. At the beginning of the emergency response, in case of damage to the communication infrastructure, the provision of communication capabilities is the first priority in the delivery of material relief.

Also, amateur radio (AR) are generally easy to repair; thus, they can be the first CS to be restored.[47] Following the 2004 tsunami, AR were the only communications link in some islands in the Indian Ocean.[10] Nongovernmental organizations carry the majority of the relief operation activities, and they suffer providing their own CS. New infrastructure-less technologies, such as ad hoc,[24] were produced to provide easy and fast communications. For example, during the New York 2001 attacks, messaging devices like RIM Blackberry were massively used to deliver messages from the WTC.[10]

CS during restoration and repair. This phase begins after the urgent life-saving operations; it is characterized by the clearance of debris from principal streets to reestablish basic transportation and communications capabilities. CSs allow better management of debris clearance, restoration of basic access to streets, more efficient information reporting, and best coordination with other efforts. Restoration of CS is relatively fast; the failure induced by congestion gradually decreases as the order is reestablished and the requests for communications are reduced. Also, providers have become very agile in their response to physical damage. After the destruction of a major switching facility in the WTC on New York attacks, AT & T's reaction was so fast that many of its vehicles were stopped at Manhattan ports of entry; even if the company was ready, the officials were not.[10]

In developed nations, where populations have easy access to technologies, CSs are an efficient tool for quickly restoring social and economic activities back to normal. The Internet has changed the way of repair and restoration functions, as it offers many alternatives to send and receive information. After the 2004 tsunami, various charities collected over $500 million via the Internet in less than 3 weeks. Released in less than 72 h, these funds could be allocated to relief efforts much quickly, as organizations had to receive funds by mail in the past.[10] During this phase, CS must be repaired quickly to support continuous relief and recovery efforts, even if it is more likely to be damaged compared with other facilities. After the New York attacks, the telephone provider was able to recover service to the New York Stock Exchange in a few days by transferring material from other sites to replace over 3 million disconnected lines.[10]

Wireless technologies are widely used to quickly recover communication services. After New York attacks, many point-to-point wireless links were used to reestablish connection of Manhattan Financial District in New Jersey and Brooklyn. These links were installed in few days and they have been widely accepted as a permanent backup.[4] Rapidly deployable cell nodes have been broadly adopted to reestablish mobile service in almost all major disasters. Also, the extended deployment of Wi-Fi with other unlicensed wireless technologies facilitates the supply of communications to critical relief operations without significant cable installations.

CS during reconstruction. This phase can be described by the restoration of people and economic activities to the same levels before calamity.[10] IT replacement is highly required during this phase because they participate significantly to support other redevelopment activities. While rebuilding cable networks can be long and costly, wireless technologies offer faster and more flexible alternatives. For example, the reconstruction of Iraq's damaged IT, after the war, underlines the benefits of using wireless technologies to reduce the time required for infrastructure replacement. The reconstruction of mobile cellular services was one of the first important contracts made by the occupation authorities.[10]

CS during redevelopment. This final step is a longer operation that may take several decades, but involves important projects for future growth and development. The transition from the previous step to the current one also offers an essential new thinking about how TN are built and managed.[10] These activities aim at preventing losses in future disasters and resolving weaknesses discovered.

Warning systems generally receive attention and major efforts to improve their efficiency. Greater attention is also given to reduce congestion in case of emergency and to prioritize calls of public officials and disaster responders. The importance of mobile networks in providing inter-organizational communication to coordinate complex response operations has induced important investments. Voice over Internet Protocol (VoIP) is essential as a mean of communication in emergencies involving the defeat of CS components or congestion. The redevelopment of CS has highlighted redundancy as an indispensable way to deal with the risk of physical damage.

Case studies, failures, and successes

In this section, we will analyze some disasters in order to identify failures and successes related to the usage of CS during extreme environments. Case studies were selected if they resulted in significant damages to human life and economic activities in affected areas. Our main criteria will be how physical destruction, disruption of supporting infrastructure, and congestion of communication infrastructures were addressed during each disaster under examination.[4,5,7,8,11,25,31,36,37,41,43,46] In the upcoming section, we will summarize important elements in a table in order to select major attributes that CSs should have to satisfy the needs of usage during extreme environments.

New York City WTC attacks, 2001

On the morning of September 11, 2001, two hijacked commercial aircraft struck the WTC towers in New York and another was flown into the Pentagon in Washington, DC. The towers of the WTC collapsed shortly after, producing many casualties and overwhelming property damage. The roof of the WTC was a major wireless site for cellular wireless services, Internet service providers (ISP), and radio-TV broadcasting services. Thus, cellular services were disrupted; ISP points-of-presence (POPs) were destroyed; and the coverage of many TV and radio stations was limited. The emergency management office for New York City, headquartered at the WTC, lost its entire command center. The loss of the command center created a major crisis for the city's overall emergency response as it was the supposed coordinator of emergency response between all agencies.

In addition, WTC building 7 collapsed and its basement power supplies were flooded, putting out of service over 1.5 million lines serving the financial district due to cuts of subscriber cables.[48] Immediately in the first few minutes after the attack, New York 911 call centers received 3000 calls. There was serious congestion of telephone networks across the east coast with New York City's mobile networks experiencing a 92% blockage rate due to high call volumes.[49] Inter-agency communications were restricted by interoperability missing between technologies. When police services realized that towers were collapsing, they ordered police to leave the site, whereas fire officials were not notified as there was little communication between the two departments. Hundreds of firefighters died when the towers collapsed because they did not receive the warning.[50]

Fortunately, a month before the attacks, the government emergency telecommunications service (GETS) became fully active with priority given to wired calls offered to national security and emergency users. Following the attacks, their success ratio was over 95%.[48] In addition, the Federal Communications Commission (FCC) had issued an order before the attack for mobile network operators to prioritize communications of officials working on emergency and security as it was done for wire lines. Unfortunately, this option was not ready. Since then, the Wireless Priority Service (WPS) has been installed to offer this service.[4] Immediately after the attack, mobile operators deployed many cellular towers on wheels to replace damaged infrastructure in order to provide critical phone services for rescue teams and other emergency governmental agencies and improve coverage in the overloaded area. The mobile service was also important as many passengers and crew members of the hijacked aircrafts made cellular phone calls to family or notified the authorities about what was happening.[49] AR was very important in facilitating communications between emergency organizations, in addition to satellite phones.[50] Also, wireless service and Wi-Fi were available in the bus that served as a mobile operations center. The Internet had not been seriously affected, even if New York had a major Internet delay. News sites such as CNN were strained; hosts became inaccessible immediately after the attacks, but the network recovered in about an hour.[49] Electricity was lost in much of lower Manhattan for almost a week, and 2 days later, backup power failed at the New York International Internet Exchange.[4] The 9/11 Commission advised creating a way for police and firefighters to communicate together during a crisis. Congress approved a law allowing the FCC to reserve many broadcast frequencies for public safety purposes. The FCC called the new network FirstNet.[48]

Indian Ocean earthquake 2004

On December 2004, a 9.0 magnitude earthquake hit the west coast of Sumatra, Indonesia, generating tsunami waves with maximum heights ranging from 2 to 30 m that began inundating coastlines of 12 countries in the Indian Ocean ranging from Indonesia to South Africa. The disaster impact was very high, becoming one of the deadliest ND, with approximately 300,000 dead and missing and 1,700,000 displaced with India, Sri Lanka, and Indonesia suffering the most extensive losses. Economic damages exceeded $13 billion, affecting many economic activities such as fishing, agriculture, and tourism, as well as physical infrastructure, residential and commercial structures, community institutions.

The disaster was so large that tsunami waves destroyed villages, roads, and a large portion of coastal infrastructure. Thus, a large amount of humanitarian aid was needed because of shortages of food and water, and economic damage.[51] Military resources were the only way to give aid to the worst damaged areas in the early stages of the crisis. While disaster response was poor, immediately following the tsunami, relief operations continued to suffer from lack of coordination. In addition, volunteers and officials were either insufficiently trained or ill-equipped to cope with such a disaster. With the high population density and tropical climate of the affected areas, avoiding epidemics became a priority. However, thanks to the quick response in providing appropriate facilities and services, this was minimized.[34]

Although this crisis was the first global Internet-mediated ND, CT were not put into their full capacity in the face of such catastrophe.[51] Therefore, the delivery of humanitarian aid went slowly due to CS failures.[31] Principal reasons for communication damages were the destruction of TI, accumulated debris, and extensive flooding that affected the power systems and cabins that contain the Base transceiver station (BTS) equipment.[43,51] In some cases, the cabins collapsed, and in other cases, the towers were damaged by waves. Furthermore, the power supply was disconnected from the main grid and complete restoration of damaged stations took many days by replacing generators, relocating cell sites, or sharing infrastructure.[43] Limited road access was the main obstacle to sending the engineering teams to fix damaged equipment and refuel the generators. In Indonesia, for example, where 67% of roads had been damaged prior to 2004, the tsunami increased the percentage of damaged roads to 72%, which hampered relief and recovery operations.[34] In addition, there were other telecommunications shortcomings such as limited network coverage, lack of disaster warning systems, and rescue equipment.

Consequently, two main objectives came into focus:[31] first, to reestablish CS to facilitate and coordinate relief operations and, second, to exchange and effectively use resource technologies, including satellites and the Internet by harmonizing activities between concerned organizations. Connectivity to all basic facilities, such as police, DM centers, and hospitals, was restored. Wireless phones and satellite communications were provided to relief organizations. After a few days, fiber optic, copper cables were fixed and telephone services were provided for free to transmit urgent information.[43]

This analysis demonstrates that thousands of deaths could have been saved if damaged countries had effective warning systems in place, but unfortunately, there was no such system.[46] Meanwhile, the Pacific Tsunami Warning Center in Hawaii detected the earthquake on the other side of the world and an alert was communicated to warning centers across the Pacific. Alerts were sent to 26 countries within 15 min after the earthquake, but it took additional minutes for alerts to be broadcast by radio and TV stations. Although the tsunami was identified, this information did not reach people at the coast because there was no established CS to deliver the warnings to the communities at risk.[34] Effectively communicating timely warnings through communications infrastructure in the developing world is a particularly challenging problem. This disaster motivated the creation of a tsunami early warning system for the Indian Ocean that became operational in the spring of 2006.[4]

As we see, failures in disasters detection have serious consequences, but false alerts also cause bad outcomes. As an example, an evacuation in Hawaii due to a false alert would cost over $68 million. Hence, for effective disaster preparedness and mitigation, many actions have been taken for disaster warning:[4,31,34,43,46,51]

- Creation of a tsunami early warning system for this zone.
- Dissemination of tsunami warnings by the installation of manned and unmanned supervision towers.
- Backing up initial warnings by AR network to transmit warning information.
- Improvement of the availability of backup power supplies.
- Use of technologies to redirect calls.
- Provision of predesigned guidelines for emergency deployment.
- Improvement of network operators' cooperation.
- Finding more resilient network architecture.
- Diversifying and backing up a principal network with the use of other CT such as AR and satellite terminals in strategic locations.
- Activation of national roaming and priority calling during disasters.
- Dissemination of alert messages through religious establishments.
- Increase participation in hazard detection by improving telecommunications access and the capacity of emergency call centers to deal with spikes in calls produced by hazards. Thus, the variation of call profiles can be an additional source to detect hazard information.
- Provision of training to help officials use their CS effectively for disaster cooperation and warning.

Haiti earthquake 2010

A catastrophic 7.0 magnitude earthquake hit Haiti on Tuesday, January 2010, causing major damage in the region. The damage was severe and catastrophic, thousands of buildings including housing, hospitals, schools, and even the parliament and many government buildings were destroyed. Unknown numbers of people were trapped; 316,000 people died; 300,000 injured; over 1,000,000 people left homeless in the streets; and 3 million people were affected.[41] Among the dead are members of parliament, many government officials, and international humanitarian workers. President Preval was saved, but he was not able to communicate with his officials as the presidential palace collapsed, and he later worked from the police headquarters. The relief operations were extremely difficult due to the loss of officials and facilities, with water and electricity completely unavailable, the transport network blocked or collapsed, and the main control tower of the airport and the main port also suffering significant damage.[52]

TI and power were severely damaged; the public telephone system was out of service and all mobile cellular providers were affected by the collapse of buildings and towers. Over 20% of cellular service provider infrastructure had collapsed.[53] International cable link and microwave connectivity were damaged. Search and rescue operations for survivors were top priority but severely constrained by damaged communications.[41] The government requested urgent relief including many medical units, electricity generators, and communications equipment to coordinate response efforts.[52]

Radio and TV broadcasts, posters, web solutions, loudspeaker trucks, and word of mouth were all used for information exchange. As a high proportion of Haitians owned mobile phones, relief operations had to find communications options based on mobile technology.[54] It was difficult for mobile network operators to provide equipment and staff to repair the damage, as they were not considered a humanitarian priority. The installation of Cells on Wheels (COWS) or Mobile System and Telescoping Antenna Array outside many telephone centrals in multiple places were used temporarily to provide communications.[53] In addition, Cisco Tactical Operations deployed much-needed networking equipment with data, voice, and wireless options. The team worked to rebuild damaged infrastructure and set up WiMAX links to back up the fiber connection until it could be repaired. This team also provided a video conference system for the government.[41] After the restoration of the service, the wide number of calls overloaded the CS; as a result, services were kept closed except to some trusted organizations.[43]

This was the globally computerized relief operation, because of the destruction and congestion of majority TI. Thus, IP communications were the unique alternative for responders to use during operations.[41] Social media and Internet tools were used for coordination and rescues, and a public web-based map was developed to share needs, as well as places where help was available in real time.[53] Donations could be made by SMS, and OpenStreetMap and Google Earth upgraded their maps to reveal updated information.[52] Facebook and Twitter were overwhelmed by demands for help.[43]

SMS was very useful to help locate and rescue victims for many reasons: it is available on any GSM network; it is one of the first services to be restored; it uses a minimum of network resources; and SMS messages can be stored on mobile phones and sent when a network becomes available.[54] Also, a system was conceived where victims could send the SMS short code 4636 including information about damages, and describe the help they needed. Messages were inputted automatically into a database, which volunteers then processed using online tools to classify and distribute information appropriately.[41] The huge number of SMS also caused network congestion and loss of service,[54] as many targeted mobile phones were not available as they had been lost or were powered off. The networks were, therefore, overloaded with large numbers of SMS messages, which could not be delivered.

Eastern Japan earthquake 2011

In March 2011, millions of people in Japan were alerted about the earthquake by mobile phone networks, radio, and TV. It occurred in the Pacific Ocean and it was the largest in Japanese history with a magnitude of 9.0. Shortly thereafter, the population was alerted about the tsunami, which was wider than expected with waves reaching a height of over 40 m and traveling 10 km past the coastline in some places. This caused catastrophic damage: about 19,000 deaths and approximately 370,000 houses were damaged. Damage was estimated at $210 billion, with nuclear power centers badly damaged and supplies of electricity, gas, and water cutoff.[4]

Fixed telephone services were severely impacted with 385 damaged buildings, 90 transport routes destroyed, and 6300 km of aerial cables and 65,000 utility poles damaged. This resulted in the deterioration of over 1.9 million landline phones, which account for around 8% of lines.[4] Damage to mobile telephone service was estimated at 29,000 mobile base stations, which represent about 22% of those in the affected region.[43] Underground facility damage was 0.3% compared to 7.9% for aerial installations.[7] The earthquake and the tsunami produced about 20% of the damage but 80% of buildings were put out of service due to power outages and the inability to refuel generators. External communications were slow due to the cutoff fiber optic and submarine cables by the tsunami. In all, 120 TV and 2 radio relay stations were also put out of service.[4]

Congestion caused usage restrictions of 80% to 90% of landline calls and 70% to 95% of mobile phone calls. The Internet was still accessible as the packet traffic restriction rate was only 0%–30%,[7] but in the hardest hit areas near the Fukushima nuclear plant, satellite phones were often the only option available to communicate.[43] Text messages were more likely to reach their destination, with some delay, as packet traffic was largely unrestricted. Social media was used extensively and Twitter was widely employed to exchange information and help people stay connected.[55]

After analyzing the causes of service interruption following the catastrophe, the Information Communication Council and many network operators proposed many solutions to improve the resilience of CS during emergency situations:[4,7,43,55]

- Use buried cables instead of aerial cables.
- Increase battery and fuel backup for important installations.

- Provide backup for important BTSs.
- Geographically distribute important CS items.
- Manage network traffic and congestion by adhering to restriction control guidelines.
- Introduce call length limits and phone calls with reduced sound quality.
- Diversify CT used such as the use of wireless and wired communication.
- Avoid network congestion by using voice message service instead of voice calls.
- Develop services and applications to share information and verify the safety of persons.
- Promote basic communications services required by relief operations and reduce the priority of other video services.
- Develop and build energy efficiency and alternative energy sources.

Nepal's earthquake 2015

On April 2015, an earthquake with a magnitude of 7.8 struck central Nepal, leaving catastrophic damage across the country. It was the largest in over 80 years to strike this country.[34] The main ground shaking lasted for 2 min and was followed by many other aftershocks in the months after the event, the biggest with a magnitude of 7.3. The human cost of the crisis was huge with more than 9100 dead and nearly 25,000 injured.[56] In addition, property damage was catastrophic: an estimated 605,254 of houses were totally destroyed; 288,255 were partially destroyed; thousands of official facilities such as schools, hospitals, and government buildings were impacted; and many historical buildings were destroyed.[57] Furthermore, it was reported that 16 hydropower facilities were significantly damaged, which represents approximately one-fifth of the total power supply. The transport network across Nepal was heavily impacted, with more than 2000 km of damage which represent 13% of the network. Many international aircrafts were diverted to airports in neighboring countries due to the level of international assistance arriving at the capital's small airport. Because of this, it took hours and days for international relief crews and equipment to arrive in Nepal. The earthquake induced significant losses in neighboring countries such as India, Tibet, and Bangladesh. The total economic cost was estimated at US$5.1 billion with additional economic losses valued at nearly US$1.9 billion for Nepal alone. This value is equivalent to more than one-third of its entire gross domestic product.[34]

Before this earthquake, the government had a history of failing to respond appropriately to the disasters and two earthquakes that hit the country in the past century, demonstrating government inefficiency. In addition, 82% of people who live in rural areas are already facing many economic, social, and health challenges; after this disaster, they found themselves even more exposed to these stresses. Nepal's geography posed significant challenges to building roads from cities to remote areas. Furthermore, cell phone reception has been essentially limited to line of sight due to hills and mountains that cover about 83% of Nepal, which often blocked cell signals. While it is possible to build repeaters to expand signal coverage, it is difficult for a poor country like Nepal to do so as it ranks 157th out of 187 countries on the United Nations' development report.[58]

In addition, daily power outages were up to 12 h a day before this crisis, despite having more than 2% of all global water resources, which could generate about 83,000 MW of hydropower; enough to turn Nepal into an electricity supplier.[59] Following the disaster, catastrophic damage to the power distribution network has kept hundreds of thousands of people in the dark. Restoration of electricity took about a month in urban cities and even longer for rural villages. This situation combined with weak country circumstances and communications challenges severely complicated recovery efforts in thousands of remote rural villages.

TI failed to successfully survive the earthquake, with damage covered cell towers, radio stations, power sources, and Internet connections. In addition, network backhaul infrastructure mainly aerially installed fiber optic cables and microwave links, and 20 of the 50 FM radio stations went off service for approximately 3 days.[60] However, the state-owned radio continued its broadcast for 24 h a day within days after the disaster, with the main focus on disaster mitigation and public service announcements. These damages obstructed the exchange of information to rural areas such as relief aid time and location and safe practices. Moreover, unpaved roads and fragile facility buildings made getting information to rural areas extremely challenging, and in some cases, word of mouth was the only means of communication. That means for isolated villages with weak signal coverage were separated not just physically but even in terms of communication. The estimated damage to the telecommunications sector was valued at $17.4 million. Unfortunately, 1 month following the earthquakes, relief efforts were still unable to contact survivors and transmit life-saving information.[61]

While the earthquakes hit everywhere indiscriminately, communications were restored ineffectively. The Nepali government did not have a plan for emergency communications to help coordinate relief workers and organizations in the face of this level of destruction. Moreover, the majority of relief operations were based in the capital city; therefore, efficient communication they needed was difficult to provide because cell towers were down and radio stations are non-functional. As this earthquake was the worst recent ND, it is important to look deeply at the use of CT during this crisis to provide a brief background of its evolution and role. The main means of communication used following the earthquake were[60–64] mobile phones ham radio, the Internet, radio, television, newspapers, and direct contact.

Mobile phones. Mobile phones were used by 92% and 84% of people in urban and rural areas, respectively. Immediately after the earthquake, use increased significantly as they were an important medium to exchange information. They were used mostly for calls, SMS, alerts, listening to the radio, accessing social media, and the Internet. Service quality degraded during disaster due to three main reasons: congestion, lack of electricity to charge mobile phones, and trouble finding places to replace cellular towers.

AR. Amateur or ham radio was very successful in connecting rescuers to survivors. Coverage was limited in Kathmandu since there are not many operators in Nepal. For future disasters, the government is working on training the police force in using this technology to back up mobile communications during disasters.

The Internet. The Internet was very useful in mostly urban areas when other means of communication was damaged. After the earthquake, Facebook and Twitter were flooded with requests for help. Moreover, The International Red Cross and tech companies introduced tools to check the safety of people online, but their effectiveness was limited by the inability to recharge devices due to power outages and Internet connectivity problems.

Radio. Before the earthquake, radio was listened by around 45% of people. Its usage was less frequent immediately after the quake, but 64% of people took action based on information received from the radio. The utilization of this service was affected by damaged radio transmitters, damaged radio sets, not owning a radio set, lack of electricity, and so on.

Television. About 42% of people in rural areas and almost 80% in urban areas have access to television. However, access to television dropped to 31% after the quake. Its use decreased for three main reasons: lack of electricity, fear of living inside the house, and television channels disseminating unreliable information.

Newspaper. Newspaper circulation is mostly limited to urban areas. During the disaster, distribution channels were lost due to damaged roads; however, many people who had access to the Internet got their news from online newspapers.

Direct contact. Around 20% of people considered direct contact as their main source of information before the earthquake. After the earthquake, it was very slow; however, it was the most trusted form of communication in rural communities. The earthquakes had destroyed many villages' roads making travel very slow and unfavorable for relief workers.

Many preparations have been made for the next disaster in light of experience:

- Installing earthquake early warning sensors, with alerts sent out using phones, radios, and sirens.[64]
- Police using AR during disasters.[61]
- Visiting and assessing the vulnerability of communications towers and rebuilding or reinforcing them as necessary.

Discussion

In Table 1, we summarized case studies according to the following criteria: causes of CS failure, affected services, used technologies, weak points and limitations, and recommendations. We chose case studies going from the beginning of the digital era, the 9/11 New York attack, to the early days of the Nepal earthquake. In addition, we selected events which caused enormous damage to human life and economic activities in affected areas including a terrorist attack, earthquakes, and tsunamis. Also, we chose countries across several continents with varying profiles of wealth, technology penetration, and development. Our aim was to diversify our samples in order to get a global background on the use of CT during HE.

The September 11 attacks were a case of a man-made extreme event in a developed country where CT was abundant. This event revealed the importance of coordination between all organizations responding to the crisis, given that improved interoperable communication could have been the key to prevent the deaths of many firefighters. Also, this crisis exposed the congestion of communication tools as an important weakness as it blocked the communication even if physical damage was not important.

The Indian tsunami is an example of a large-scale event that hit many countries, which are mainly underdeveloped with already weak communications and transportation infrastructure. Main weaknesses were revealed such as the lack of an efficient early warning system and advanced CT, and the inefficiency of regional and international cooperation in the communication of warning information and response. Although it was one of the deadliest event with very high

Table 1. Summary of disaster case studies.

	New York City World Trade Center attacks, 2001	Indian Ocean earthquake, 2004	Haiti earthquake, 2010	Eastern Japan earthquake, 2011	Nepal earthquake, 2015
Causes of CS failure	- Destruction - Power outage - Congestion	- Destruction - Power outage - Congestion - Flooding - Lack of fuel - Road damage - Debris	- Hard destruction - Power outage - Congestion - Road damage - Loss of personnel	- Destruction - Power outage - Congestion - Road damage - Lack of fuel	- Destruction - Power outage - Road damage - Weak infrastructure
Affected services	- Radio, TV - Fixed - Wireless - ISP	- Radio, TV - Fixed - Wireless	- Wired - Wireless - Submarine cables	- Radio, TV - Wired - Wireless - Submarine cables	- Radio, TV - Wired - Wireless
Used technologies	- Amateur radio - Satellite phones - Wi-Fi - COWS - Mobile - Wireless links	- Internet - Satellite phones - Mobile	- Radio, TV - Internet - Social media - SMS - Web applications - COWS - WiMAX	- Internet - Social media - Satellite phones - SMS - Mobile	- Radio, TV - Mobile - Amateur radio - Internet - Social media
Weak points and limitations	- Interoperability	- Warning system - Lack of training - No established communications	- Lack of resources	- Aerial cables - Dependence on nuclear energy	- Governance - Lack of resources - Geography - Rural population - Low signal coverage - Lack of unpaved roads - Lack of planning
Recommendations	- Call and traffic prioritization - Common broadcast frequencies	- Creation of a tsunami early warning system - Amateur radio - Predesigned guidelines - Topologies change from series type to ring - Backing up principal CS - Improve call centers - Improve cooperation	- Disaster resilient infrastructures	- Promote buried cables - More batteries and fuel - Backup CS - Geographical distribution of CS - Advanced call and traffic management - Diversify CS technologies	- Early warning system - Amateur radio - Disaster efficient infrastructures

CS: communications systems; ISP: Internet service providers; COWS: Cells on Wheels; SMS: short message service.

Table 2. Damages to communication networks during examined disasters.

	New York 2001	Indian Ocean 2004	Haiti 2010	Japan 2011	Nepal 2015
Congestion	●	●	●	●	●
Physical damage	◖	●	●	●	●
Disruption of supporting infrastructure	○	●	●	●	●

● Fully applies ◖ Partially applies ○ Does not apply

economic losses, the impact could have been reduced if the warning information had been communicated quickly to the coastal population. Even though the earthquake was detected, the tsunami was not detected in time; thus, people were not able to benefit from the time difference between the earthquake and the tsunami to seek safety. Even if the tsunami had been identified, early warning information did not reach the coastal population because there was no established CS to deliver warnings to the communities at risk. This is a common and larger problem affecting all underdeveloped countries in the world.

The Haiti earthquake is an example of a large-scale extreme event that hit a poor country, in which damage was severe and catastrophic, with electricity, water, transportation, and communication completely disrupted. Coordination was particularly difficult because many Haitian government officials, parliament members, and international aid personnel died. This event was the first mostly information data-driven relief response, due to the destruction and congestion of the majority of communication facilities, so IP communication was the only option for the responder to use as the core of the response. Internet and social networking applications, like Facebook and Twitter, were used to provide rescue and coordinate operations. SMS messages were used to help locate victims and to make donations. Web-based maps were developed to share needs and places where help was available. Also, OpenStreetMap and Google Earth revised their maps to reflect up-to-date disaster information.

The Japan earthquake was a three-in-one disaster, with an earthquake, tsunami, and nuclear crisis at the same time. It is the biggest earthquake in Japan's history and provides an example of how a developed country dealt with such a situation in the digital era. The earthquake was detected and the tsunami warning system alerted people shortly after. Nuclear power plants, TV and radio stations, fixed and mobile telephone services, and external communications were severely damaged. Congestion caused high usage restrictions, and text messages were more likely to reach their destination. Proposed technical solutions issued at the end of this crisis can be used all around the world for efficient disaster preparedness and response.

The last case was the 2015 earthquake in Nepal, which was the largest in over 80 years to strike the country. The earthquake hit everywhere indiscriminately, leaving catastrophic damage across the country; the human and economic cost was huge. Infrastructure, transport, facilities, and communications were damaged. This crisis was a typical case of a governmental failure during extreme events: communication was restored ineffectively, daily power outages were up to 12 h before this crisis, and the large rural population was already badly linked to the capital where the majority of relief operations were based. Also, hills and mountains, which cover about 83% of Nepal's land, posed significant challenges to building roads and often blocked wireless communication signals.

In Table 2, major damages that may occur to CS during examined extreme events are outlined. In the majority of extreme events, loss of electricity and lack of fuel for generators have been principal reasons for losing communication by putting telecommunications equipment out of service. So, it is important to provide an autonomous power supply and enough fuel for generators as electricity failure may last for a long time. Also in the majority of disasters, significant damage occurred to infrastructure. Thus, installing equipment in safe places where they are far from risk may decrease the failure of CS. For example, putting equipment in physically higher locations and avoiding basements could reduce the effects of flooding. Also, the use of aerial facilities or cables should be avoided in favor of buried solutions, and critical equipment should be as geographically dispersed as possible. Moreover, communications providers should ensure redundancy and backups for critical systems, in addition to implementing interoperable systems and diversified access technologies such as satellite, TETRA, GSM, and WiMAX. Diversity must include multiple backhaul link by using satellite, wireless, and undersea cables in order to preserve connectivity if principal link fails. Operators need to embrace mesh topologies to provide redundancy routes and reduce the risk of network failure.

The impact of extreme events is different between rural areas and cities. For example, transportation within metropolitan zones hit by a disaster can be difficult, making the shipment of communication equipment impossible in the majority of cases. To address this risk, resilient telecommunication towers can be built in some strategic locations. In small cities or rural areas, infrastructure installed could be rebuilt in its original location, or a more accessible location could be chosen. The human impact varies depending on age, disability, and language with elderly and disabled people being particularly vulnerable as they require assistance in taking the right action during the crisis in their own language. Impact also varies depending on the country, where developed countries have better infrastructure, technology, communications, management, and preparedness utilities, which reduce human loss and facilitate life-saving action. In contrast, poverty and poor governance in less developed countries hamper the effective mobilization and use of all available alternatives.

TN congestion is mainly caused by calls made by affected people asking for emergency relief, or trying to contact relatives. Therefore, it is necessary to use some tactics to alleviate congestion such as increasing network resources; diversifying communication means; reducing call hold times and sound quality; designing CS architectures that can deal with traffic surges; implementing congestion control algorithms for the Internet to reduce load during congestion; prioritizing the use of some applications and services that require less bandwidth such as SMS and email restricting the use of video streaming for urgent use only; giving special privileges to some users, such as relief organizations to make calls during disaster situations; and using packet-based communication like the Internet.

In the beginning, the use of IT was limited for relief organization. In a very short amount of time, technology has exploded and the use of the Internet and social media like Facebook and Twitter is widespread during extreme events to facilitate rescues and coordination. Public and private entities concerned with response activities are broadly deploying DM software. Web-based maps and applications were developed to share road conditions and places where help was available in real time. SMS is a powerful tool to exchange information as it can reach its destination during congestion due to the low bandwidth required; making a donation and sharing location and other information are efficient applications based on SMS during crisis time.

In some cases, loss and damage could be avoided if an efficient warning system were available. A warning system requires sensors to monitor, and provide digital data about environmental circumstances that help predict events such as earthquakes or tsunamis within a specified margin of error. It is important to diversify means of dissemination of alerts and public information after a disaster. For this aim, we can use many means, such as TV or radio, mobile networks by cell broadcast service, social media or web services, sirens or loudspeakers, and video screens, in public places to inform people about hazards or other information such as evacuation procedures. In other words, warning or emergency information must be as close as possible and as easily reachable as possible to vulnerable populations for efficient DM. The time elapsed between detection of extreme event signs and the event itself is the time when the existence of a convenient warning system can be effective. This time differs according to the type of hazard to detect from tens of seconds for earthquakes to hours or weeks for hurricanes. The impact of early warnings may vary on the local, regional, or global scale. The coordination of early warning system operations requires a network of establishments or organizations. The importance of an efficient warning system is well known in order to preserve communities, lives, and infrastructure.

Attributes and characteristics

Inadequate CS capabilities can have catastrophic consequences on extreme events response efficiency, and data exchange during challenging conditions.[5] Communications during extreme events require high performance, resilience, flexibility, message prioritization, fast delivery, and other capabilities that we will detail in this section. Depending on the type of extreme event, its context, and concerned individuals, weaknesses of CS can be quite different and actions taken to protect life and property can be different also; for example, a fire alarm's siren is not sufficient in a deaf school. However a CS that is able to operate during extreme conditions will be able to performe very well in normal conditions. The deployment of CS during HE must fulfill some specifications in order to offer and preserve reliable communications services.[13] Generally, the best-known requirements for CS during hard conditions mentioned in the literature and that we can deduce in light of previous case studies are as follows:[13,23,30,36,65–68]

- Robustness and reliability: This is the ability of CS to provide and maintain core functions and services just as it would perform in normal circumstances. To do so, CS must supply basic services in challenging environments and afford quick service restoration. Also, CS should be robust against certain node failures, since the reception of certain information in a timely and accurate manner can be critical to saving human lives. For example, data-driven communication, like the Internet, proved markedly robust against congestion.

- Provided service: Voice is the principal service of a traditional CS. However, individuals may also need to exchange maps, images, and other relevant data in addition to having an Internet connection and real-time transmission. Furthermore, in specific cases and for rescue purposes, it might be recommended to support video streaming.
- Automation: Automatic organization and optimization help decrease the human contribution in CS administration and enhance its reliability. Also, it may minimize the time needed for initial configuration or manual reconfiguration if environmental conditions change. Furthermore, system topology can be adjustable, and bandwidth is allocated according to the need of users.
- Mobility: This condition concerns the mobility of users and the network itself. Mobile infrastructure may facilitate deployment, optimization, and installation of the CS. Also, system architecture can be adapted to the concerned area or in order to improve performance. User mobility also allows for emergency personnel to communicate while moving within the damaged zone, as disasters may affect wide geographical areas.
- Interoperability: The deployed CS should be compatible with various technologies in order to expand the covered zone and diversify available services when needed. This attribute is also very essential for information exchange between different organizations, as each one may have its own equipment. In this way, individuals may be able to transparently connect and exchange data through substituted infrastructure regardless of the technology they have. For example, IP networks can be used as a communication protocol between various emergency teams.[65]
- Rapid deployment: As relief personnel are most concerned with reducing the number of victims, CS planning is mostly done on the fly and it is far from being formalized. Thus, the deployment process must be simple and easy with no need for specialized personnel or complex procedures. Equipment must be tolerant of the harsh environment and rapidly deployable, which involves rude manipulation due to the lack of time required for rescue operations.
- Scalability: This is the ability of CS to expand geographical coverage and the number of users supported efficiently. Therefore, CS must be automated to avoid service disruption in case of environmental change.
- QoS: This is the ability to prioritize and categorize traffic, such that high priority traffic gets priority to guarantee delivery of urgent messages in case of congestion. QoS also includes parameters such as availability, throughput, latency, jitter, and error rate. Depending on compatible services, the network may support video streams and live audio with adequate requirements. For example, VoIP calls may require a maximum packet delay of 100 ms, jitter of less than 30 ms, and packet loss of less than 1%.[12]
- Security: Multiple agencies and possibly military forces may be implied in the disaster response. Therefore, sensitive data crossing CS could be exposed and should be appropriately protected and encrypted.[28] This level of security guarantees that only authorized persons can access the information, and each entity receives the information intended for it only. For example, medical records should be available to the medical teams only. Security can also include data integrity, authentication, and access control.[2]
- Cost: CS cost should be reasonable for deployment, maintenance, and equipment. As resources are mostly used during basic and essential life-saving activities, low-cost CS can be easily deployed in low-resource developing countries.
- Energy Efficiency: CS should be designed to work as energy efficiently as possible in order to keep the system's infrastructure available for a long time. As we have already seen in our case studies, power outages are common in the majority of disasters due to infrastructure damage, fuel shortage, or simply battery discharge. An efficient energy system can last longer in such circumstances, most importantly during the golden first 72 h.
- Localization: The current location of a user can be required for emergency context; therefore, a CS must have the ability to automatically obtain the current location of its users.
- Popularity: Popular technologies such as cellular could be used because most people are accustomed to them. They have to be user-friendly as relief personnel and victims are more focused on life-saving activities. Furthermore, popularity allows for the possibility of deployment with less training or technical expertise, which is beneficial as human resources are less available in the damaged area in the immediate aftermath of a disaster.
- Capacity: The CS must support a sufficient number of users and overcome traffic congestion.
- Coverage: This is the ability of CS to cover a wide area without the need to deploy many points of presence. This property can be

characterized by the maximum distance a user can reach while still connected. The coverage can reduce the cost and time of system deployment by reducing the amount of infrastructure required to cover the damaged area.

Conclusion and future work

The relevance of CS is undeniable for information exchange and operations coordination during HE, in order to prevent damage to human life and economic activities. Moreover, if CSs are designed so that they are able to operate with a good QoS during challenging conditions, their operation in normal conditions will be more robust and reliable. At the beginning of this work, we gave an extensive introduction to the reciprocal effect of HE and CT on each other. Also, we examined related work and how QoS of CS may fail or decrease, and the effect of this failure on human life in general and extreme events response. Then, we studied how communications are used during HE and gave an overview of the main weaknesses and limitations that CSs may suffer based on many case studies. Also, we detailed relevant attributes that CSs should have to perform well. These attributes will be useful in our future research to select best-suited CT for a good communication QoS. A deep understanding of CS behavior during HE, such as smart cities, rural areas or disasters, is essential to design or select more resilient technologies that are able to operate well in challenging conditions and perform with a good QoS during normal environments. In future work, we will continue our search for reliable CS and address some of weaknesses found during this article by comparing most relevant modern CT without prior judgment of which one is best fitted. A framework to select the right CT according to relevant attributes of a special application or service will be proposed.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Sahu S. *Guidebook on technologies for disaster preparedness and mitigation*. New Delhi, Delhi: Asian and Pacific Centre for Transfer of Technology (APCTT).
2. Channa MI and Ahmed KM. Emergency response communications and associated security challenges. *Int J Netw Secur Appl* 2010; 2: 179–192.
3. Kishorbhaia VY and Vasantbhai NN. AON: a survey on emergency communication systems during a catastrophic disaster. In: *7th international conference on advances in computing & communications, ICACC-2017*, 22–24 August 2017, Cochin, India, https://www.sciencedirect.com/science/article/pii/S1877050917319993
4. *Technical report on telecommunications and disaster mitigation*, Version 1.0, 06/2013. Geneva: ITU-T Telecommunication Standardization Sector of ITU, ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery, 2013.
5. Dealing with disasters: technical challenges for mobile operators. GSMA Disaster Response, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Dealing-with-Disasters_Final.pdf
6. Bridging the digital divide: a case study of a collaboration between a metropolitan municipality and a non-profit organization, http://scholar.sun.ac.za/handle/10019.1/100879
7. *Maintaining communications capabilities during major natural disasters and other emergency situations final report*. Study Group on Maintaining Communications Capabilities during Major Natural Disasters and other Emergency Situations, 27 December 2011, http://www.soumu.go.jp/main_content/000146938.pdf
8. The Associated Press-NORC Center for Public Affairs Research with Funding from the Rockefeller Foundation. *Communication during disaster response and recovery*, 2013, http://www.apnorc.org/PDFs/Resilience%20in%20Superstorm%20Sandy/Communications_Final.pdf
9. East Asia Summit Earthquake Risk Reduction Center, National Institute of Disaster Management. *Disaster communication*. New Delhi, India: East Asia Summit Earthquake Risk Reduction Center, National Institute of Disaster Management, 2013.
10. Townsend AM and Moss ML. *Telecommunications infrastructure in disasters: preparing cities for crisis communications*. New York: Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service, New York University, April 2005.
11. Lieser P, Alvarez F, Gardner-Stephen P, et al. Architecture for responsive emergency communications networks. In: *Proceedings of the 7th global humanitarian technology conference (GHTC)*, 2017. New York: IEEE, https://ieeexplore.ieee.org/document/8239239
12. Saim G, Paul S, Sreenan Cormac J, et al. Cognitive radio for disaster response networks: survey, potential, and challenges. *Wirel Commun* 2014; 21: 70–80.
13. Miranda K, Molinaro A and Razafindralambo T. A survey on rapidly deployable solutions for post-disaster networks. *IEEE Commun Mag* 2016; 54: 117–123.
14. Premkumar R and Jain R. Wireless networks for disaster relief, current issues in wireless and mobile networking, white paper, 30 April 2014, Washington, DC, https://

www.cse.wustl.edu/~jain/cse574-14/ftp/disaster/index.html
15. Ferris E and Petz D. *The year that shook the rich: a review of natural disasters in 2011*. London: Brookings-Bern Project on Internal Displacement, 2012.
16. Marchetti N. *Telecommunications in disaster areas*. Aalborg: River Publishers Series in Communications, 2010.
17. Rautela P and Pande RK. Implications of ignoring the old disaster management plans: lessons learned from the Amparav tragedy of 23 September 2004 in the Nainital district of Uttaranchal (India). *Disaster Prev Manag* 2005; 14: 388–394.
18. Schryen G and Wex F. Risk reduction in natural disaster management through information systems: a literature review and an IS design science research agenda. *Int J Inform Syst Crisis Res Manage* 2014; 6: 38–64.
19. Brown S and Mickelson A. A decision framework for choosing telecommunication technologies in limited-resource settings. *Future Internet* 2018; 10: 8.
20. Fragkiadakis A, Ioannis A, Elias T, et al. Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks. *Eurasip J Wirel Commun Netw*. 2011; 2011: 13.
21. Gomes T, Tapolcai J, Esposito C, et al. A survey of strategies for communication networks to protect against large-scale natural disasters. In: *2016 8th international workshop on resilient networks design and modeling (RNDM)*, Halmstad, 2016, pp. 11–22, https://ieeexplore.ieee.org/document/7608263
22. Bartolacci NR, Aubrecht C, and Aubrecht DO. A portable base station optimization model for wireless infrastructure deployment in disaster planning and management. In: *Proceedings of the 11th international ISCRAM conference* (ed Hiltz SR, Pfaff MS, Plotnick L, et al.), University Park, PA, 1 May 2014. University Park, PA: The Pennsylvania State University.
23. Wang W, Xu Y and Khanna M. A survey on the communication architectures in smart grid. *Comput Netw* 2011; 55: 3604–3629.
24. Srinivasarao D, Devi Pradeep P and Bammidi A. A survey of emergency communication network architectures. *Int J u- e-Serv Sci Technol* 2015; 8: 61–68.
25. Leah Davis G and Robbin A. Network disaster response effectiveness: the case of ICTs and Hurricane Katrina. *J Homel Secur Emerg* 2015; 12. DOI: 10.1515/jhsem-2014-0087.
26. Markakis EK, Politis I, Lykourgiotis A, et al. Efficient next generation emergency communications over multi-access edge computing. *IEEE Commun Mag* 2017; 55: 92–97.
27. Dial N, Fear M, Ferrill M, et al. Fuzhou University: emergency disaster preparedness. Technical report. *University of Southern California, Los Angeles, CA*, June 2016.
28. Li Y. *A survey on communication networks in emergency warning systems*. Report No. WUCSE-2011-100, 2011. Saint Louis, MO: All Computer Science and Engineering Research.
29. Roser M and Ritchie H. Natural catastrophes, 2018, https://ourworldindata.org/natural-catastrophes
30. Huang J-S, Lien Y-N and Hu C-L. Design of contingency cellular network. In: *2012 14th Asia-Pacific network operations and management symposium (APNOMS)*, Seoul, 2012, pp. 1–4, https://ieeexplore.ieee.org/document/635 6074
31. Samarajiva R. Mobilizing information and communications technologies for effective disaster warning: lessons from the 2004 tsunami. *New Media Soc* 2005; 7: 731–747.
32. Chen BX. F.C.C. seeks ways to keep phones alive in a storm. *The New York Times*, 5 February 2013, https://bits.blogs.nytimes.com/2013/02/05/f-c-c-revisits-communications-failures-after-hurricane-sandy/
33. Mckay J. Sandy created a black hole of communication, 28 January 2013, http://www.govtech.com/em/disaster/Sandy-Black-Hole-of-Communication.html
34. Benfield A. *2015 Nepal Earthquake*. AccessScience, n.d.: n.p., Thought leadership. Aon Plc, 1 September 2015.
35. Richards C. When communications infrastructure fails during a disaster. *Disaster Recovery Journal*, 2015, https://www.drj.com/articles/online-exclusive/when-communications-infrastructure-fails-during-a-disaster.html
36. Cole J and Hawker E. *Emergency services communications resilience for the twenty-first century*. London: Royal United Services Institute, February 2014.
37. Burroughs JE. *Tree factors leading to the failure of communications in emergency situations*. PhD Dissertation, College of Social and Behavioral Sciences, Walden University, Minneapolis, MN, 2017.
38. Nowell B and Steelman T. Communication under fire: the role of embeddedness in the emergence and efficacy of disaster response communication networks. *J Publ Adm Res Theor* 2015; 25: 929–952.
39. Verkuil PR and Fountain JE. The administrative conference of the United States: recommendations to advance cross-agency collaboration under the GPRA Modernization Act. *Public Administration Review* 2014; 74: 10–11.
40. de León V, Carlos J, Bogardi JJ, et al. Early warning systems in the context of disaster risk management. *Entwickl Ländl Raum* 2006; 40: 23–25.
41. Nelson C, Steckler B and Stamberger J. The evolution of hastily formed networks for disaster response technologies case studies and future trends. In: *Proceedings of the IEEE global humanitarian technology Conference*, 2011, https://ieeexplore.ieee.org/document/6103680
42. Menon VG, Pathrose JP and Priya J. Ensuring reliable communication in disaster recovery operations with reliable routing technique. *Mob Inf Syst* 2016; 2016: 9141329.
43. Samarajiva R and Zuhyle S. *The resilience of ICT infrastructure and its role during disasters*. Bangkok: United Nations Economic and Social Commission for Asia and the Pacific, 2013.
44. United Nations Economic and Social Commission for Asia and the Pacific. *Note by the Secretariat: enhancing regional cooperation on disaster risk reduction in Asia and the Pacific, information, communications and space technologies for disaster risk reduction* (First session). Bangkok: United Nations Economic and Social Commission for Asia and the Pacific, Committee on Disaster Risk Reduction, 25–27 March 2009 https://www.unisdr.org/files/resolutions/B090859.pdf
45. Khawaja WS and Lu X. Utilization of telecom technologies for the disaster management in underdeveloped

coastal districts of Pakistan. *Int J Acad Res Bus Soc Sci* 2013; 3: 197–213.
46. A newsletter of and for the community of disaster risk management practitioners and development workers. In: *Emergency communications for disaster management*, January–April 2007, Vol. 13, no. 1, http://www.acade mia.edu/2390563/Emergency_Communications_for_Disaster_Management
47. Cid V, Mitz A and Arnesen S. Keeping communications flowing during large-scale disasters: leveraging amateur radio innovations for disaster medicine. *Disaster Med Public Health Prep* 2018; 12: 257–264.
48. Noam EM. *What the World Trade Center attack has shown us about our communications networks*. New York: Columbia Institute for Tele-Information, Columbia University, http://www.citi.columbia.edu/elinoam/articles/What_the_World_Trade.pdf
49. Pittman E. *Little progress on national public safety network 10 years after 9/11*. Government Technology, http://www.govtech.com/public-safety/National-Public-Safety-Network-10-Years-After-911.html
50. Brito J. *Sending out an S.O.S.: public safety communications interoperability as a collective action problem*. Arlington, VA: Mercatus Publications, 2007.
51. Pettit S, Beresford A, Whiting M, et al. The 2004 Thailand tsunami and the April 2012 tsunami warning were lessons learned? In: *Humanitarian logistics*, http://orca.cf.ac.uk/70835/
52. Margesson R and Taft-Morales M. *Haiti earthquake: crisis and response*. Washington, DC: Congressional Research Service, 2 February 2010.
53. DesRoches R, Comerio M, Eberhard M, et al. Overview of the 2010 Haiti Earthquake, Earthquake Engineering Research Institute. *Earthq Spectra* 2011; 27: S1–S21.
54. Rogers A. Haiti case study, July 2018, http://www.ifrc.org/fr/what-we-do/beneficiary-communications/haiti-case-study/
55. Peary BDM, Shaw R and Takeuchi Y. Utilization of social media in the East Japan Earthquake and Tsunami and its effectiveness. *J Nat Disaster Sci* 2012; 34: 3–18.
56. Cook ADB and Zin Bo Htet MS. *International response to 2015 Nepal Earthquake lessons and observations*. NTS Report No. 4, October 2016, https://www.rsis.edu.sg/wp-content/uploads/2016/10/NTS_Report_4_Nepal_final_04Oct2016.pdf
57. Sanderson D and Ramalingam B. *Nepal earthquake response: lessons for operational agencies*. London: Active Learning Network for Accountability and Performance in Humanitarian Action (ALNAP), 2015.
58. Adhikari A, Hassett B, Lamsal R, et al. *Nepal's 2015 Earthquake: communication and the marginalization of Dalits*. Worcester, MA: Worcester Polytechnic Institute, 3 May 2016.
59. Ribeiro J. Nepal communications hit by power outage, last-mile issues. *ComputerWorld*, 27 April 2015, https://www.networkworld.com/article/2915014/internet-of-things/nepal-communications-hit-by-power-outage-last-mile-issues.html
60. Joel L. Narratives from Nepal: relief and rebuilding after the Gorkha Earthquake. *Earth Magazine*, 6 December 2015, https://www.earthmagazine.org/article/narratives-nepal-relief-and-rebuilding-after-gorkha-earthquake
61. Sakzewski E. Nepal Earthquake: damage to last years for hard-hit rural communities, as aid provided in Kathmandu. *ABC News*, 27 April 2015, https://www.abc.net.au/news/2015-04-27/nepal-earthquake-rural-areas-to-suffer-lasting-effects/6424266
62. Danielle P. How social media is helping Nepal rebuild after two big earthquakes. *Quartz India*, 19 May 2015, https://qz.com/india/406562/how-social-media-is-helping-nepal-rebuild-after-two-big-earthquakes-2/
63. Dougherty D, murphy O, Sharma S, et al. National media landscape 2014, Nepal opinion survey Wave III, Internews, September 2014.
64. Humanitarian Country Team, Communicating with Communities Working Group: Nepal Earthquake 2015, inter-agency common feedback project, March 2016.
65. Iapichino G, Bonnet C, del Rio Herrero O, et al. Advanced hybrid satellite and terrestrial system architecture for emergency mobile communications. In: *26th international communications satellite systems conference (ICSSC)*, San Diego, CA, 10–12 June 2008, http://www.eurecom.fr/en/publication/2417/detail/advanced-hybrid-satellite-and-terrestrial-system-architecture-for-emergency-mobile-communications
66. Lehmann A, Paguem Tchinda A and Trick U. Optimization of wireless disaster network through network virtualization. In: *Proceedings of the eleventh international network conference (INC 2016)*, https://www.e-technik. org/aufsaetze_vortraege/aufsaetze/lehmann_et_al_inc2016 .pdf
67. Wozniak S and Schaefer G. Towards information services for disaster relief based on mobile social networking. In: *Proceedings of the 6th future security research conference*, Berlin, September 2011.
68. Maryam H, Shah M, Javaid Q, et al. A survey on smartphones systems for emergency management (SPSEM). *Int J Adv Comput Sci Appl* 2016; 7: 301–311.