INTERNATIONAL HELLENIC UNIVERSITY

DEPARTMENT OF INFORMATION AND ELECTRONIC ENGINEERING

MSc IN WEB INTELLIGENCE

Study of communication technologies for prediction and mitigation of man-made disasters and emergency situations

MASTER'S THESIS

OF

ALEXANDROS GIANNOPOULOS

Supervisor: Periklis Chatzimisios
Professor, International Hellenic University

Thessaloniki, September 2021

Η σελίδα αυτή είναι σκόπιμα λευκή.

INTERNATIONAL HELLENIC UNIVERSITY

Department of Information and Electronic Engineering I.H.U.
MSc IN WEB INTELLIGENCE

Study of communication technologies for prediction and mitigation of man-made disasters and emergency situations

MASTER'S THESIS

OF

ALEXANROS GIANNOPOULOS

Supervisor: Periklis Chatzimisios
Professor, International Hellenic University

Approved by the three-member selection board at 2/10/2021.

(Signature)	*(Signature)*	*(Signature)*
....	....	....
Name Surname	Name Surname	Name Surname
Professor, I.H.U.	Professor, I.H.U.	Professor, I.H.U.

Thessaloniki, September 2021

(Signature)

....

Alexandros Giannopoulos

BSc Applied Informatics in Management and Economy, Technological Educational Institute of Western Greece

Περίληψη

Η παρούσα διπλωματική εργασία έχει ως αντικείμενο την μελέτη των τεχνολογιών επικοινωνίας για την αντιμετώπιση καταστροφών (φυσικών και ανθρωπογενών) με έμφαση στη δεύτερη κατηγορία. Επιπλέον, υπάρχει ιδιαίτερη μνεία στις τεχνολογίες επικοινωνίας για την αντιμετώπιση και πρόληψη εκτάκτων καταστάσεων. Πιο συγκεκριμένα έγινε λεπτομερής αναφορά στις φυσικές και ανθρωπογενείς καταστροφές όπως και στους χρήστες και τις εφαρμογές τεχνολογιών επικοινωνίας σε έκτακτα περιστατικά. Στην συνέχεια αναλύθηκαν λεπτομερώς μια σειρά από υπάρχουσες και ανερχόμενες τεχνολογίες οι οποίες χρησιμοποιούνται από τις υπηρεσίες πολιτικής προστασίας. Ακόμα, αναφέρθηκαν τεχνολογίες επικοινωνίας σε συγκεκριμένες περιπτώσεις ανθρωπογενών καταστροφών και περιπτώσεις υπηρεσιών πολιτικής προστασίας. Επιπροσθέτως γίνεται αναφορά σε έναν μεγάλο αριθμό προκλήσεων που προκύπτουν και διαδραματίζουν σημαντικό ρόλο για την ομαλή λειτουργία και υλοποίηση των τεχνολογιών επικοινωνίας σε περιπτώσεις έκτακτης ανάγκης. Τέλος η παρούσα διπλωματική αναφέρεται στην ανάγκη για υλοποίηση και εύρεση νέων τεχνολογιών επικοινωνίας έτσι ώστε όλες οι υπηρεσίες πολιτικής προστασίας να προσφέρουν τις υπηρεσίες τους στο κοινό με τον καλύτερο δυνατό και ωφέλιμο τρόπο. Επιπλέον αναφέρεται στην ανάγκη για αρμονική συνεργασία των διαφορετικών τεχνολογιών επικοινωνίας αλλά και διαφορετικών υπηρεσιών πολιτικής προστασίας κατά την διάρκεια κρίσεων. Τέλος, αναφέρονται λεπτομερώς σημαντικά συμπεράσματα τα οποία είναι βασισμένα στην βιβλιογραφική έρευνα και αφορούν τις δυσκολίες αφομοίωσης νέων τεχνολογιών, την συνύπαρξη διαφόρων τεχνολογιών επικοινωνίας αλλά και την συνεργασία διαφορετικών υπηρεσιών πολιτικής προστασίας.

Λέξεις Κλειδιά:

Δίκτυα Πολιτικής Προστασίας, τεχνολογίες επικοινωνίας, ανθρωπογενείς καταστροφές, φυσικές καταστροφές, 5G, Διαδίκτυο των Πραγμάτων, διαχείριση καταστροφών

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

The main objective of this M.Sc. thesis is the research and study of upcoming communication technologies for prediction and management of disasters (natural & man-made), especially focusing on the latter ones. In addition, the current thesis addresses communication technologies for monitoring and prediction in emergency situations. Furthermore, we discuss about natural and man-made disasters as well as critical communication technologies and their end users. A number of communication technologies, techniques and hardware used by public safety agencies is discussed in detail too. Moreover, communication technologies and technologies used by public safety agencies in specific use-cases are discussed in detail. Furthermore, the current thesis emphasizes on a number of challenges and open issues referring to establishment and operation of communication technologies during emergency situations. In addition, the current thesis explains the urgent matter of researching new communication technologies so that public safety agencies can provide their services more efficiently. Finally, the thesis discusses important conclusions that are based on scientific research after evaluating a number of communication technologies and public safety agencies needs.

Keywords: Public Safety Networks, communication technologies ,man-made disasters, natural disasters, 5G , Internet of Things (IoT), disaster management

Η σελίδα αυτή είναι σκόπιμα λευκή.

Table of contents

List of figures

List of tables

List of abbreviations

PS	Public Safety
EMS	Emergency Medical Services
AI	Artificial Intelligence
WSN	Wireless Sensor Networks
FC	Fog Computing
IoT	Internet of Things
AIoT	Artificial Internet of Things
PSN	Public Safety Network
MEC	Mobile Edge Computing
NS	Network Slicing
UAV	Unmanned Aerial Vehicles
SON	Self Organizing Network
NFV	Network Function Visualization
DMC	Disaster Management Cycle
PAN	Personal Area Network
D2D	Device to Device
M2M	Machine to Machine
CR	Cognitive Radio
BDEM	Big Data and Emergency Management
V2V	Vehicle to Vehicle
DL	Deep Learning
ML	Machine Learning
QoS	Quality of Service
SAR	Synthetic Aperture Radar
DCNN	Deep Convolutional Neural Network
LEA	Law Enforcement Agency
DM	Data Mining
GIS	Geographic Information System
DoS	Denial of Service
CM	Crime Mapping
LMR	Land Mobile Radio

1 Introduction

1.1 Disasters & climate change

We can define a disaster as a "*sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community's or society's ability to cope using its own resources*" [1]. Although disasters can be caused by nature (natural disasters), they can also have human origins (man-made disasters).Some examples of natural disasters may include earthquakes, droughts and floods. On the other hand, some examples of man-made disasters may include oil spills and nuclear disasters.

The climate change of our planet has brought tremendous effects in the area of natural disasters as well as their frequency and severity. Furthermore, human reckless activity for many years is part responsible we witness natural disasters being more severe and unpredictable. Recent research has shown that climate change will bring an increase in strength and frequency of natural disasters. One example is droughts and storms. With increasing global surface temperatures, the possibility of more droughts and increased intensity of storms will likely occur. As more water vapor is evaporated into the atmosphere it becomes fuel for more powerful storms to develop [2]. In addition, rising sea levels as an effect of climate change can lead to the exposure of locations to the force of sea and its high waves (tsunamis).

1.2 Man-made disasters

The current thesis is addressing both categories of disasters (natural and man-made), but mainly focuses on man-made disasters like nuclear and oil spill accidents. We emphasize to current and upcoming (state-of-the-art) technologies as well as their role in prevention, response, preparedness and mitigation of such disasters. Communication technologies used by public safety users are included too. Moreover, we discuss in detail how technologies and communication techniques changed the way public safety agencies confront man-made disasters. To conclude with, we refer to the human factor and its negative role in the frequency and complexity of man-made disasters.

1.3 Critical communications & disaster management

Before emphasizing to Public Safety Networks (PSNs) terms like critical communication and disaster management will be explained for better understanding of the topic. Critical communications include telecommunication systems and devices that must provide reliable and secure communication at all times [3]. Currently, critical communications are the spine of functioning for emergency services. Disaster management can be defined as the organization and management of resources and responsibilities for dealing with all humanitarian aspects of emergencies, in particular preparedness, response and recovery in order to lessen the impact of disasters [4] (Figure 1.1).

1.4 Public Safety Networks

Before moving on discussing about the services that should be supported by the PSNs, it is important clarifying that a PSN is the communication network used by officials such as police officers, firefighters and healthcare personnel to coordinate their operations [5].

1.4.1 Types of Services that should be supported by PSNs

In this Section we refer to all the types of services that should be supported by PSNs. These may include voice, data and multimedia services. All of these services will be discussed in detail as follows.

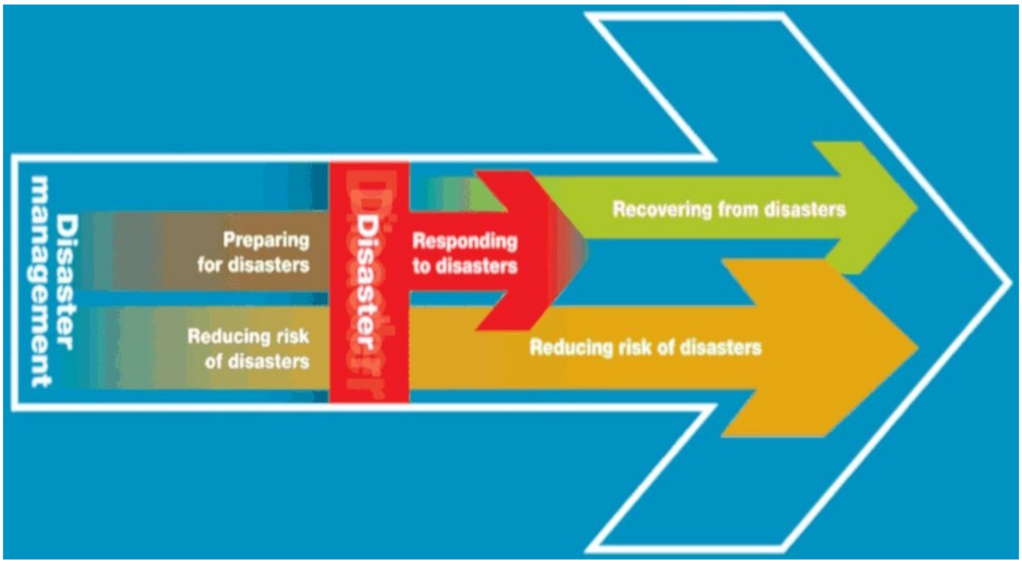

Figure1.1:Disaster management [4]

Voice services

A PSN should support a variety of voice services in order to be efficient. These voice services include:

- Individual call: One to one basic voice communication between two public safety users.
- Group call: One - to - many calls. Initiated by one public safety user to others in a group.
- Acknowledged group call: Similar to group calls with one basic difference. In order to be achieved, caller must receive a sufficient amount of acknowledgements.
- Broadcast call: Similar to group call. The difference in this case is that communication is unidirectional. Calling user broadcasts and other users just listen.

Data services

They are divided into two main categories, namely Short Data Services (SDS) and Packet Data Services (PDS). SDS can be used for individual or group messages. Messages are sent instantly making the communication extremely efficient. On the other hand, PDS may be a connection-oriented or a connectionless packet data service [8]. They establish a connection between the source and destination and deliver the data needed.

Multimedia Services

Multimedia services supported by PSNs can include a combination of two or more media components such as voice, data video and still image [6]. Multimedia services supported by a PSN may also include video streaming, video on demand and images.

1.5 Thesis Overview

The current thesis is structured as follows. In Chapter 2 we analyze the users of public safety communication technologies as well as public safety applications. Furthermore, we refer to the technical requirements of critical communications and their characteristics. Moreover, the second Chapter analyzes various techniques PSNs use and the hardware which is used by public safety authorities.

In Chapter 3 we discuss about the evolution of communication technologies PSNs use until the current 5th generation (5G). Furthermore, this Chapter includes an overview of cellular technologies for public safety.

Chapter 4 discusses in detail various use cases and scenarios in which public safety communication technologies are used. Moreover, the chapter refers to disaster management cycle and its importance.

Chapter 5 refers to the challenges and open issues of utilizing communication technologies for public safety needs. To conclude with, in Chapter 6 discusses important conclusions which are based on scientific research after evaluating communication technologies and the needs of public safety agencies.

2 Background

2.1 Users of Public Safety

In this Section we will discuss about the users of Public Safety Networks (PSNs). Throughout the world a vast number of agencies use PSNs in order to minimize possible human casualties during calamities. The use of PSNs by public safety agencies gives them the opportunity of emergency response in critical situations. Some of these users/agencies are:

a. Police Departments

One important public safety authority is Police and its departments. The main obligation of police officers is law enforcement. They serve and protect civilians and their main goal is to keep communities safe. Along with paramedics and firefighters, police is one of the most important public safety agencies.

b. Fire Departments

Fire departments are obliged to protect life and property and their main objective is extinguishing of fires either large or small in scale. In case of large scale fire incidents, public safety authorities and most importantly fire departments need to communicate fast and efficient. Nowadays, Fire departments (especially in USA) use public safety platforms like FirstNet for communication and coordination purposes. Using this kind of platforms increases the efficiency as well as the cooperation of Fire departments with other public safety services.

c. Emergency Medical Services (EMS)

First Responders are the first medical service to arrive in critical situations. Main purpose of EMS is to provide care to victims during calamities and emergency situations. We usually consider as first responders law enforcement officers, paramedics and firefighters. First responders depend on digital and connected technologies to quickly provide life-saving assistance, deal with crisis situations, and bring order to chaotic situations [7]. Technology is improving rapidly and there are several technology trends that are digitally aiding medical care services as shown in Figure 2.1.

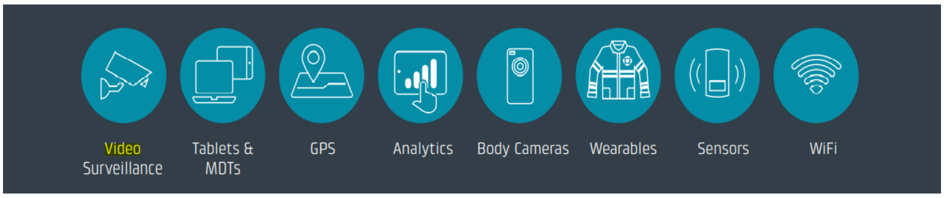

Figure 2.1: Trends in First responders Connected Technologies [7]

d. Coast Guard, ocean rescue, shore safety, border protection,

A Coast Guard is a maritime security organization. This public safety agency protects ports and coasts from all kinds of dangers. A typical Coast Guard, in the areas mentioned above, provides safety and security to the people; protects the marine transportation system and infrastructure and maintains the territorial integrity [8]. The main public safety communication method of Coast Guard is the Very High Frequency (VHF) radio, a two-way communication technique. Another PSN used by Coast Guard is Rescue 21, an advanced maritime Computing, Command, Control, and direction-finding Communications (C4) system designed to better locate mariners in distress and save lives and property at sea and on rivers [8]. Coast guard officers are obliged to respond in natural disaster incidents too. For this reason their means of communication must be adaptable and dynamically configurable.

Ocean rescue is one more organization which is using public PSNs. In addition, ocean rescue is an expert team of first responders including Emergency Medical Technicians (EMTs) and Paramedics which specialize in preventative actions, ocean rescues and emergency medical assistance [9]. The main objectives of shore safety are the reduction of drowning individuals and the perseverance of safety in the shores and beaches. These objectives require the use of PSNs.

Border Protection (BP) agency of every nation includes a variety of obligations. Some of their main objectives are the enforcing of customs and detection/prevention of terrorists and terrorist weapons. One more obligation of a border protection agency is the prevention of illegal trafficking of people and narcotics. In order to achieve these objectives BP is another public safety agency which is using PSNs.

e. Military

The army of every nation is a powerful fighting force serving by land, sea and air. It has as its main objective the perseverance of peace and defense from foreign and domestic enemies. In order to achieve this, armies all around the world use PSNs to communicate more efficiently and cooperate with other public safety authorities during critical incidents. For instance US army has chosen FirstNet as its main public safety communication platform following the fire and police departments of USA.

f. Individual /Personnel

Not only public safety authorities use PSNs but also common people as individuals. Individuals use public safety systems by their initiative in critical and serious incidents. This way they find valuable information about critical situations and seek ways to secure their lives. In recent years public safety agencies urge people to use public safety systems in order to gather information about a site of a disaster. This way with the valuable aid of civilians, public safety agencies take better decisions and gain situational awareness. Decisions may include evacuation plans or mitigation/response methods.

2.2 Critical communications for Public Safety applications

In this Section we will discuss about public safety applications and their valuable aid to public safety agencies and first responders. We will also analyze the technical requirements needed for the applications to operate. To conclude with, we will discuss about the critical communication characteristics.

2.2.1 Public Safety applications

In order for public safety agencies to provide their services more efficiently and quickly they use a number of public safety applications. These applications include a variety of state-of-the-art technologies. In recent years public safety applications evolved rapidly. With the aid of these applications public safety officers are in position to do things way faster and more accurate. There are applications specifically designed for the needs for almost every public safety agency. Particularly, police and Fire departments are in position of locating the position of their officers using GPS as a location tracking technology which is embedded in their radios and visualize it on an electronic map. The electronic map is situated in the departments.

Furthermore, Police officers can read license plates from remote locations with a local app. They just program cameras in parking areas to snap license plates or ask officers on patrol to take the picture with a handheld device [10]. They even have the ability to compare license plates with the help of an app. Another useful application which is used by police officers is background check application, officers simply type up the personal information of a civilian into a form on their handheld device and see results in seconds. To conclude with, police officers are in place to scan driver’s license and fingerprints with the help of an application which is connected to the database of their department.

Moreover, EMS are in place to transmit data via an application to the hospital in critical situations for example the current health status of an inbound patient. In fire and rescue critical situations one efficient solution that has been proposed is SAFECommand app [11]. It securely shares critical information with those operational resources that need it - whether on the incident ground to incident commanders, control room staff or mobile resources. Officers in the field with the help of this app get fresh information even without real-time connection.

In acts of terrorism, public safety agencies use applications for facial recognition on people. These apps are directly connected to their database of their departments. Moreover, Tactilon Agnet [12] is another public safety application that brings a revolution to the communication of public safety agencies and their communication capabilities. It can be downloaded to your smartphone like any other commercial application. With Tactilon Agnet downloaded on your smartphone, you can also talk or send messages to people who carry a professional radio or communicate with the central control and command room. Moreover, it carries a variety of features like instant messaging, video communication and location mapping.

2.2.2 Critical communication technical requirements

Public safety agencies need to communicate and coordinate with precision in order to provide their services. They need resilient and dependable mission critical communication technologies. However, in order for these communications technologies to be effective they need to meet a number of requirements. Some of them are the following [13]:

- Efficient group communications: A group call is an important feature in professional communications. Moreover, a group call helps public safety users to communicate and coordinate with each other. Every public safety agency must have one group call for their particular needs. On the other hand, when officers from different organizations need to communicate and cooperate, share the same group call and coordinate a common emergency response.
- Fast and reliable connection: Public safety organizations need steady and reliable connection in order to deliver efficiently their services. Furthermore, governments created dedicated public safety networks especially for the needs of public safety. Dedicated networks ensure availability and minimize the risk of a communication failure. We call a network available when public safety users can access its resources when they need them.
- Prioritization: Prioritize of public safety data ensures the safe delivery of critical information. Communication of public safety officers must be on top of the communication chain. This means their communication needs must be prioritized over the communication needs of individuals. Furthermore, priorities must be given among mission critical users. Certain users and teams have more critical data to share than common population, so their communications must have different priorities.

2.2.3 Critical communication characteristics

PSNs consist of special features and designed especially for the public safety user needs. Some typical examples of these characteristics are [8]:

- Features specified by public safety users: Majority of critical communication characteristics are defined by public safety users and their special requirements.
- Performance: Taking into account the fact that usage pattern of PSNs is extremely unpredictable, in case of a sudden loss of network they have to perform to the outmost level without any further problems. This is the reason why capacity and latency of PSNs are designed to perform in the worst-case scenarios.
- Live access to critical data: It is vital for public safety users to have live access on data for instance reports or images from disasters sites.
- Broadband data rates: This feature applies mainly to LTE networks. The idea is that the network supports broadband data rates to allow public safety agencies to exchange in real time critical information such as high-definition video, graphics, photos, and high-fidelity audio, etc.
- Availability: A PSN and its services must always be available to public safety users no matter the difficulties that may occur.
- Reliability: It is one of the top characteristics of PSNs. No matter the extreme weather conditions or the destruction of the current network infrastructure a PSN must always be able to provide its services to the public safety officers.
- Security: An important characteristic that all PSNs should include. Security means encryption of data of public safety users and of course the data they exchange during critical incidents.
- Location/ awareness: A PSN must be in a position to help first responders collect relevant data depending on the critical situation. Sensors and a GPS system aid a PSN in order to achieve this.
- Situational awareness: An important feature which allows the exchange of important data between first responders and public safety departments. This way both parties analyze the situation better and collaborate in a better level.
- Devices: Public safety users have in their position a large variety of devices to aid them in order to provide their services. These devices can be either hands free or implemented in vehicles. They carry technologies such as LTE, 3G, 4G and Wi-Fi.
- Power consumption of devices: A feature of PSNs which allows batteries of devices to last longer. Furthermore, it optimizes their battery life through a duty cycle which contains functions such as transmission, speak and standby. A very critical feature especially during calamites and serious incidents.

2.3 *Technologies*

In this Section we will discuss about technologies and communication technologies used by public safety agencies based on their coverage distance. In addition, we will refer to the current standards with narrowband and broadband connectivity and their networks as well as their communication techniques and hardware (equipment) they use. To conclude with, we will discuss about the use cases these technologies can be deployed.

2.3.1 Standards with Narrowband Connectivity

Private Mobile Radios (PMRs) use a variety of narrowband technologies in order to operate [14]. PMRs are widely used among public safety agencies as they provide first responders with services such as private group calls and push-to-talk. PMRs are dedicated communication networks designed for improved reliability and availability. Since they are dedicated to the professional organization that deploys them, PMR networks deliver high quality of service in a reliable, continuous and secure way. However, they are designed for specific coverage needs. In addition, narrowband standards fail to handle a significant amount of data because of the very narrow bandwidth of channels which restricts data rates. Furthermore, they have long been reserved for critical voice communication among public safety organizations but currently experiencing expansion with 4G and 5G technologies to enhance their coverage. Standards which PMRs are based on are Project 25, TETRA, TETRAPOL and DMR (Digital Mobile Radio).Project 25 is a standard developed by the Telecommunications Industry Association (TIA) as TIA-102 Project 25. TETRA is a standard developed by the European Telecommunications Standards Institute (ETSI). TETRAPOL is a digital PMR standard developed by another industry group in Europe [8]. To conclude with, DMR is another communication technology standardized by ETSI.

2.3.2 Standards with Broadband Connectivity

The advantages public safety agencies could gain from broadband communication technologies are countless. Furthermore, broadband communication standards offer features such as larger bandwidth and higher data rates. Public safety organizations using broadband communication are in position to handle a significant amount of data with ease comparing to narrowband standards. To conclude with, some of the broadband standards are Wi-Fi, WiMAX and LTE. Both Wi-Fi and WiMAX are standardized by the Institute of Electrical and Electronics Engineers (IEEE) [8]. On the other hand, LTE and LTE-A (Advanced) are the only accepted broadband communication technologies worldwide for the 4th generation of mobile broadband communication technologies.

2.3.3 Related Communication Standards & Networks

In this Section we will discuss about related communication standards and networks used by public safety organizations.

2.3.3.1 Networks

Starting on with the area of networks, there are few examples worth mentioning.

(i)WMNs (Wireless Mesh Networks) / WSNs (Wireless Sensor Networks)

Wireless Mesh Networks (WMNs) are extremely helpful to first responders. Moreover, they provide connectivity for emergency vehicles. Some of the advantages of WMNs are self-configuration, fast and easy deployment and low installation cost. WMNs can provide wireless network coverage of large areas without relying on a wired backbone infrastructure or dedicated access points [15]. In addition, they give access to mobile users to a fixed network infrastructure. Figure 2.2 depicts a typical example of a WMN network.

On the other hand, Wireless Sensor Networks (WSNs) are widely used by public safety organizations for monitoring natural hazards such as floods and wildfires. WSNs consist of a large number of pocket-sized sensors deployed in autonomous manner in the area under surveillance [16]. Some of the main features of WSNs are:

- Collection of real-time data.
- They perform specialized tasks depending on the demands.
- Limited energy resources.
- They are extremely sensitive to noise.
- Low maintenance and installation cost.

Furthermore, WSNs are also used in other areas like smart agriculture and healthcare. They are used to gain knowledge via surveillance of vital characteristics such as temperature, motions and vibration. However, WSNs face a large number of challenges. The most important of them are security attacks. WSNs are extremely vulnerable to malicious attacks and there is a big danger for corruption of data their nodes are carrying.

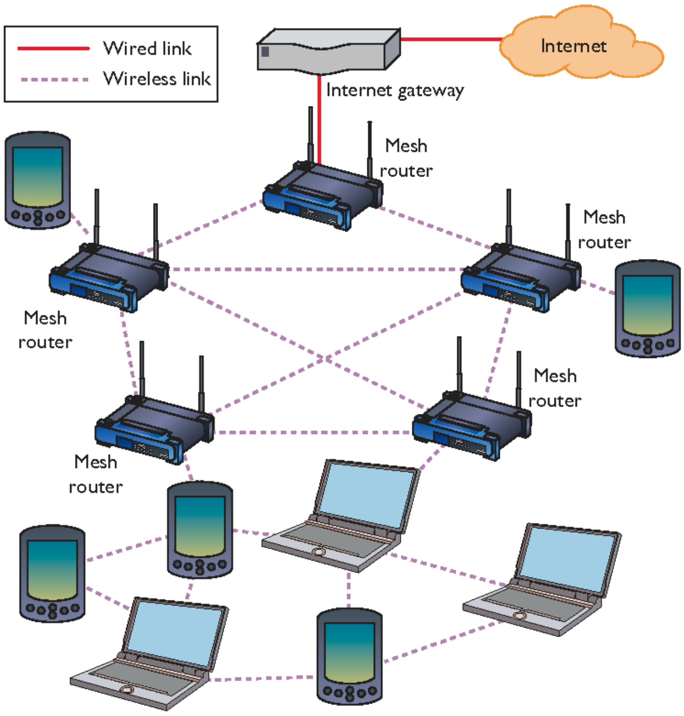

Figure 2.2: Typical example of a WMN [15]

(ii) LPWAN (low-power wide-area network) (LoRa, SigFox, NB-IoT)

Low-power wide-area networking technologies (LPWAN) are in position of handling large-scale applications of smart grids. LPWAN offers important features for its applications such as delay tolerance, lower power consumption and low data rates. One of the major applications of LPWANs is public safety. LPWANs can be used for detection and monitoring of fires, river flood monitoring and public safety management. In addition, low data rates make LPWAN a good option for IoT applications. In addition, LoRaWAN which uses Long Range (LoRa) as its modulation technique is one of the most promising LPWAN technologies. LoRa is able to provide long range communications to its users. LoRa uses a symmetric key cryptography to ensure security to its devices [17]. In addition, LoRa uses a number of topologies for its networks like star and mesh. LoRa devices are connected to LoRa gateways. Gateways are connected to the server and the servers are connected to the internet. In Figure 2.3 we see a typical LoRa network architecture.

On the other hand, SigFox is one of the most interesting subsets of LPWAN technologies [18]. This technology transmits data. The amount transmission data depends on the geographical place the communication technology is established. Furthermore, SigFox provides low power and low-cost communication devices. In Figure 2.4 we can see a typical SigFox network architecture.

Another famous LPWAN technology is Narrowband Internet of Things (NB-IoT). It means NB-IoT technology acts in narrow-band for IoT solution such as E-health, smart agriculture, smart city, energy and utilities, retail, and smart home [18]. A top feature of NB-IoT is low power consumption. In Figure 2.5 we can see a typical NB-IoT network architecture.

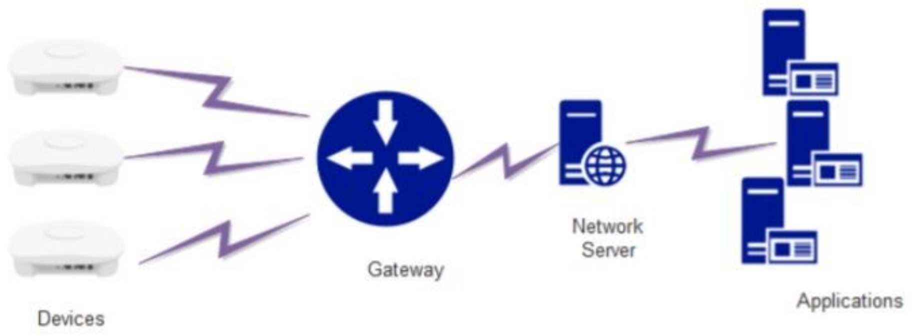

Figure 2.3: LoRa Network architecture [17]

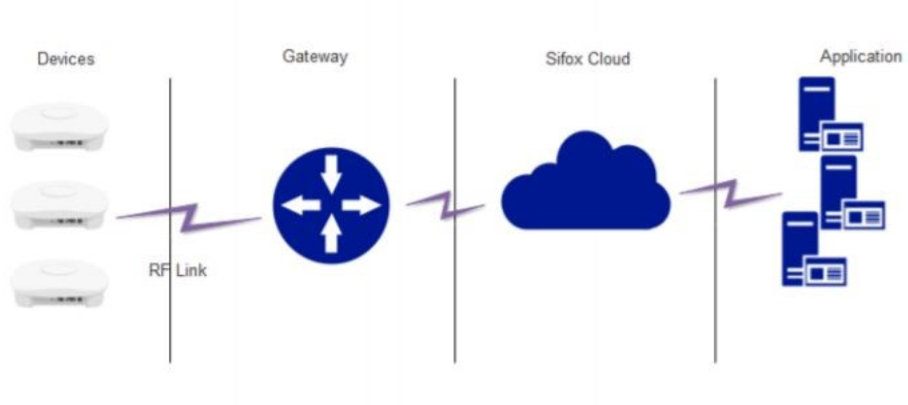

Figure 2.4: SigFox Network Architecture [17]

Figure 2.5: NB-IoT Network architecture [17]

(iii) WiMAX - IEE 802.16

Worldwide Interoperability for Microwave Access (WiMAX) is a broadband network which has as its top main features the provision of a low-cost network to public safety organizations with capabilities equal to 3G and 4G public wireless networks. WiMAX was developed to resolve all the WiFi issues for the public safety industry. In other words we can assume that WiMAX is an upgrade of WiFi specifically developed for public safety needs and requirements. In addition, research has shown that a WiMAX network can support applications that can help law enforcement [19]. WiMAX includes several advantages and drawbacks shown in Table 2.1 [20].

WiMAX	
ADVANTAGES	**DISADVANTAGES**
• Bigger range than WiFi systems • Applicability to dedicated public safety spectrum that is not shared with the public at large. • Higher data rate which include voice, data and video services.	• Current developments of the mobile WiMAX standard are not consistent with the fixed standard making compatibility an issue. • Still in development • Adaptability

Table 2.1: Advantages and disadvantages of WiMAX [19]

(iv) PANs (Personal Area Networks - 6LoWPAN)

Personal Area Networks (PANs) are extremely valuable for public safety organizations. They are able to connect different kinds of devices first responders carry. Furthermore, PANs can create small scale communication networks for emergency responders by utilizing portable devices and/or sensors. PANs greatest strength is its data transmission--a capability that not only helps first responders to communicate but save lives [21]. In addition, PANs are in position of enhancing situational awareness by providing information to public safety agencies. Information may include for instance floor plans or burning buildings.

Furthermore,(IPv6 over Low-power Wireless Personal Area Networks) or commonly known as 6loWPAN is a PAN standard. In addition, 6LoWPAN is the main competitor of ZigBee, another standard of PANs.6LoWPAN offers interoperability with other wireless 802.15.4 devices as well as with devices on any other IP network link (e.g., Ethernet or Wi-Fi) with a simple bridge device [22].

(v) WPANs (Wireless Personal Area Networks - Bluetooth, ZigBee)

Wireless Personal Area Networks (WPANs) can be used for public safety communication needs. In addition, WPANs applications were originally conceived as low power, short range (under 10 meters) wireless communications among ad hoc groups of devices to eliminate cables [23]. Both Bluetooth (802.15.1) and ZigBee (802.15.4) are standards for WPANs. Bluetooth was originally created for commercial purposes for communication including voice and data transferring and computing devices. Bluetooth can also be used by public safety organizations as it offers several advantages. Some of them are:

- Quality of Service (QoS)
- Low power consumption
- High level of security
- Low cost of maintenance
- Peer to peer networking

On the other hand, ZigBee technology, one of the most popular technologies in the field of WSN, gradually becomes a dispensable part of people's life [24]. Lots of companies and public safety organizations choose ZigBee as their standard due to its flexible characteristics like low-cost and security. Furthermore, public safety agencies use the ZigBee standard for safety monitoring systems.

(vi) WANET/MANET (Wireless Ad hoc NETwork, Mobile Ad hoc NETwork)

Wireless Ad hoc NETworks (WANET) are used by public safety organizations mostly because they are designed to connect two or more wireless devices without requiring a network infrastructure or equipment for instance a router or an access point. In addition, they have a set of special characteristics. They require minimal configuration and can be deployed quickly, which makes them suitable for emergencies, such as natural disasters or military conflicts [25].

On the other hand, Mobile ad hoc Network (MANET) is a set of nodes, which are basically distributed spatially and communicating each other wirelessly and here smart things can communicate with each other remotely[26].MANET has the ability to establish an autonomous network in disaster sites using satellite links. This is the reason why MANET is commonly used by public safety agencies, as it gives them the opportunity for clear and quick communication. In other words, MANETs can be quickly deployed, operated and controlled by the public safety organizations during operations, putting them in a position of confidence and of being completely in control of their own communication resources [27]. Both MANET and WANET are Self Organizing Networks (SONs) with characteristics like self - configuration, self-forming and self-healing.

(vii) VANETs (Vehicular Ad hoc NETworks)

Vehicular ad hoc networks aid public safety agencies in multiple ways. One particular way is monitoring and controlling traffic by using different communication nodes. It is a SON which and has the ability of self-configuration and a high level of adaptability. In addition, it is important to mention that VANETs are increasing their efficiency if they are used in a smart grid. They can be used as intelligent transportation systems (ITS). Vehicles act as carriers of wireless transceivers. Furthermore, already VANET is well established to monitor and control vehicular traffic using the concept of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. Moreover, VANET shares similar features with MANET. In other words VANET is a sub-type of MANET. In addition, VANET comparing to MANET offers a better mobility of nodes. Better mobility of nodes offers more efficient communication for public safety users. We refer as nodes to both vehicles and base-stations infrastructure. To conclude with, VANETs are applicable to a number of safety applications. Some of them are [28]:

- Public safety: Warning message to the driver of a vehicle for an approaching emergency vehicle.
- Collision avoidance: A warning message is sent to vehicles so they take a necessary action to avoid a car accident.
- Communication between Vehicles: This application involves the V2V communication for exchange of information between vehicles about the various events like forward collision warning, road condition warning etc.
- Vehicle problem: This VANET safety application sends a warning message to drivers for possible fault within the vehicle.

(viii) SPANs (Smartphone ad hoc networks - WiFi, WiFi direct)

Smartphone ad hoc networks (SPANs) are extremely helpful to public safety organizations. They are ad hoc networks that use smartphones. In addition, a group of smartphones close in range can cooperate and create an ad hoc network. In order to create networks they use the existing available hardware such as WiFi. Furthermore, they use multi hop routing and for this reason they differ from traditional networks such as WiFi direct. On the other hand, WiFi direct supports single hop routing.

Some of the applications of SPANs in public safety can be:

- Creation of a dynamic network when there is no current infrastructure to use.
- SPANs can also be used during critical situations like natural disasters or terrorist attacks when current infrastructure is unavailable or partially destroyed.

2.3.3.2 Hardware

In this Section we will discuss in detail the current hardware which is used by public safety agencies and organizations.

(i) End user devices

In order for public safety agencies to provide their services efficiently, they use a number of end user devices. In addition, end user devices are extremely valuable for critical communication and transferring data among public safety users. Some typical examples of end user devices are [8]:

- Mobile radios: They are installed in vehicles such as cars or motorcycles. They are a heavier than portable radios mainly because they are attached to the vehicles. We can see a mobile radio in Figure 2.6.
- Portable radios are always carried (handheld) by the users. Therefore, they are relatively small and lightweight. A portable radio is illustrated in Figure 2.7
- Dispatch consoles: Systems that are used by public safety officers to locate end user devices.

Figure 2.6: Typical examples of portable radios [8]

Figure 2.7: Example of a Mobile radio device [8]

(ii) Wearables

Public safety officers use many devices and gadgets in order to provide their services quickly and with precision. Moreover, evolution of technology brought groundbreaking technologies which made a huge difference to the way first responders operate. Research has shown that wearable tech improves rapidly situational awareness of first responders. In addition, wearables such as smart watches have the ability to receive and send critical data to Police departments. By this way police officers can protect the public more efficiently and respond to various unpredictable critical situations.

Furthermore, for public safety agencies, wearable devices offer a new way to connect police officers to Computer-Aided Dispatch (CAD), detect signs of distress and potentially save lives [29]. Smart watches have the ability of silently alerting police officers for upcoming critical data and most importantly they can connect to other applications. This gives first responders the feeling of a full situational awareness on the scene. Moreover, Samsung a popular company for its smart phones and gadgets, claims that its product the Galaxy Watch is ready for public safety use – it can be used to monitor the user's heart rate, location tracking and display images and alerts[30].

Another important gadget which can make a difference in the area of public safety is smart glasses. In the not-so-distant future, smart glasses can work as powerful platforms which run applications in a similar way to smartphones [30]. Furthermore, the main challenge is about the creation of these applications with functions designed especially for public safety needs. Moreover, public safety officers are currently using body-worn camera systems. These systems have a number of features rather than just recording. Some smart body-worn camera systems can include automated transcription, Wi-Fi connectivity and other solutions to help with storing and processing the large amount of video data [31].

(iii) UAVs

Nowadays drones or UAVs gained mass popularity in various use cases and scenarios. In addition, we can witness the use of drones in more and more cases. One of them is public safety. Moreover, UAVs have countless remarkable abilities which can aid public safety officers. The benefits that drones can enable for public safety officials are as numerous as they are powerful, with the potential to do everything from gather info about a fire to find a missing person quicker to ensure officers are not putting themselves in harm's way [32]. Furthermore, firefighters can use drone technology to observe and set boundaries to wildfires. Drones can also enable wireless communication in order to enhance connectivity among public safety users. Moreover, they have the ability to go in dangerous areas and operate where humans cannot.

If drones are placed correctly during large-scale disasters, they can rapidly increase their operation efficiency. The placement of UAVs can provide a flexible and promising services for public safety officers as shown in Figure 2.7 [33]. However, UAVs still face a number of challenges during the design process. The most important of them is the efficient utilization of energy because that affects the complete performance of the UAVs [34]. Environmental parameters, flight time duration, payload and real-time deployment altitude are the basic constraints that also affect the consumption of energy [35].

(iv) Sensors

Public safety users have a lot of equipment and technologies to use in their disposal in order to provide their services with precision and efficiency. Nowadays, sensors have gained popularity in the area of public safety. Moreover, a particular example is the use of body-worn sensors from firefighters. Body worn sensors are available with technologies such as LTE, WiFi and Bluetooth. Often a dedicated device with a single purpose, wearables and sensors can provide beneficial functions such as authentication, heart rate monitoring, video recording, hands-free communication, or location tracking[36].Particularly, wearable body sensors for firefighters can detect distress and gather data like heat temperature. Moreover, an EMS employee in a hazardous environment is utilizing multiple wearable devices and sensors to monitor their health status (e.g., blood pressure, heart rate, respiration, temperature, blood oxygen, head orientation, external temperature, and environment information, including air quality readings) and enable voice communication [36].

In addition, body-worn sensors can aid firefighters by computing the heat risk for hot environments. Sensors also have the ability to measure skin and body-core temperature. Furthermore, they allow users to set upper and lower thresholds for body temperature, heart and breathing rate and combine this with a red/amber/green alert index [37]. We can see a typical example of a body-worn sensor in Figure 2.8.

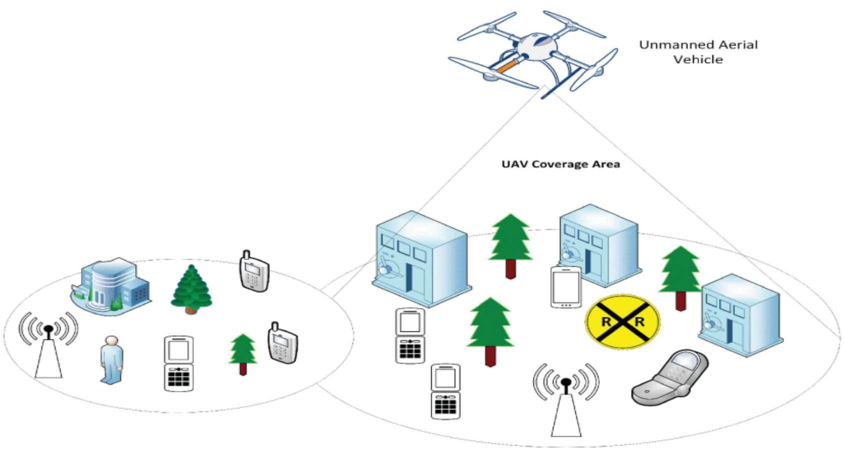

Figure 2.8: Public safety services of UAVs [33]

Figure 2.9: Body-worn sensor for public safety users [37]

(v) Robotics

The massive evolution of robotic technology has made it a powerful ally of public safety agencies in order to constrain natural disasters or confront emergency situations. Robots have the ability to interact with the physical word unlike other technologies. Moreover, robots, just like other complex systems such as cars, airplanes, and manufacturing facilities, require longer times to adapt, deploy, and make reliable than many software applications [38]. Robotic technologies are inherently programmable, and robots have been adapted and deployed, to various use cases of public safety.

With the current pandemic crisis robotic technologies could prove to be extra helpful for healthcare and public safety. First of all, they can be used to carry touchless sensors for vital signs which can collect vital measurements from the patients. Secondly, they are able to clean and disinfect areas without demanding human presence. This way human life is preserved from the danger of being infected from the virus. Furthermore, robots can take temperature, blood pressure, capture sounds such as coughing and can even perform basic imaging functions (e.g. ultrasound) and perform sample collection (e.g., nose swabbing, phlebotomy) [36].

In other areas of public safety robots are being used for patrolling as well as search and rescue missions. Some of the key features robotic technologies offering to public safety are [39]:

- Sharing of information and exchange of digital evidence based on blockchain.
- Threat detection
- Video streaming
- Detection capabilities for early identification of criminal activities and hazardous incidents.

- Data collection from disaster sites
- Quick response in order to minimize human casualties and environmental damage.
- Providing resilient communication in the field for public safety users.

2.3.3.3 Techniques

In this Section we will discuss about a number of techniques and technologies public safety agencies use in order to provide their services.

(i)Software Defined Networks (SDNs)

In order for 5G networks to lower their latency, increase their reliability and assure more capacity combine a set of technologies. One of them is Software Defined Networks (SDN). SDN technology has the ability to enhance PSN communication methods. Moreover, SDN is the new trend in PSNs referring to network management and control. Primary goal of a SDN is to bring to the networks the software flexibility and scalability that will allow them to better fulfill the upcoming needs of network operators and their users [40].Today's networks have become so complex that it was necessary to rethink their design and simplify the way they operate. In addition, PSNs need to have a level of fault tolerance and priority management. The generalization of the software approach in networking with SDN permits the design of new generation of PSNs in an elegant way [40]. SDN separates the data-plane, composed of the various devices, and the control-plane which includes the network control logic. In order to achieve this, SDN uses a technology which is called OpenFlow. In addition, OpenFlow can enable efficient priority management for PSNs. OpenFlow network decisions are decided on a flow basis, for arbitrary flow definition, and implemented in the form of rules with priority levels [40]. Furthermore, flows are treated differently depending the policies of each country a PSN operates. To conclude with, OpenFlow ensures the strict respect of such policies.

(ii) Network Function Virtualization (NFV)

Primary goal of Network Function Virtualization (NFV) is the enhancement of communication efficiency of networks, in our case PSNs. Moreover, we can refer to NFV as the replacement of the current network hardware with virtual machines (VMs). These VMs have the ability to use a hypervisor to run networking software and processes such as routing and load balancing [41]. A NFV separates communication services from dedicated hardware, for instance routers. In addition, this gives the vital ability to a PSN to upgrade dynamically without demanding installation of new hardware. It is important to mention that services which run on virtual machines can run on less expensive servers. The implementation of NFV offers PSNs a number of advantages such as [41]:

- Fewer appliances: Because NFV runs on virtual machines instead of physical machines, fewer appliances are necessary and operational costs are lower.
- Scalability: When the network architecture is scaled with VMs it becomes faster and easier to use. Furthermore, it does not require the purchase of further hardware.

On the other hand, the use of NFV includes a number of risks. Malware is difficult to isolate within the VMs and network traffic becomes less transparent. Moreover, virtualizing network components increases their vulnerability to new kinds of attacks compared to physical equipment that is locked in a data center [41].

(iii) Network Slicing (NS)

The term network slicing is a design technique for building and managing a network that meets the requirements of its users. The way to achieve a sliced network is to transform it into a set of logical networks on top of a shared infrastructure [42]. Each logical network serves a predefined purpose. One of the top benefits of network slicing not only in public safety area but in business models too is that it provides service flexibility and ability to deliver services faster with high security and more efficient. PSNs such as Firstnet are dedicated networks for first responder communication during disasters. However, these networks face challenges such as the increasing data traffic and users. Furthermore, these challenges force PSNs to increase their capacity in order to deliver their services efficiently.

For these reasons, governments enabled “Public Safety Slices” based on network slicing technology. The main idea is to quickly develop and deliver dedicated PSNs to first responders outside the current operating PSNs such as FirstNet. The main goal is the relief of current overused PSNs. An adoption of a Public Safety Slice rather than building dedicated networks from the beginning not only saves cost, but also provides flexibility and options for public safety customers [43]. The latest network slicing standard is Release 16 of 3GPP and is already in the disposal of public safety organizations to use.

(iv) Blockchain

Blockchain technology refers to a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system [44]. It is extremely helpful for public safety agencies such as police departments to implement technologies such as blockchain. Furthermore, blockchain technology holds the potential to help transform public safety by improving the way agencies handle their most sensitive evidence and data, enhancing interagency cooperation and promoting greater public trust in the integrity of investigations [45]. In addition, blockchain is a decentralized database shared across a network, in our case a PSN. Blockchain technology provides a way to incorporate a variety of data from multiple sources, anonymize it, track it and ensure its authenticity without the need for third-party validation. The public-safety implications of such a technology are enormous [45]. To conclude with, critical information public safety users exchange is more than valuable during disasters, blockchain technology is the answer of ensuring the integrity and authenticity of them.

(v) Artificial Intelligence (AI)

The popularity of Artificial Intelligence (AI)is increasing rapidly and is used in many cases. One of them is public safety. AI technology has been systematically used by public safety agencies in the area of decision making. Governments have long been using computer algorithms like AI to assist government officials make decisions and increasingly to automate those decisions without human involvement [46]. Furthermore, governments are also deploying AI to upgrade public safety and security. AI is also used to identify real-time patterns for enabling emergency response in case of cyber attacks.AI can enhance operational effectiveness through automation and augmentation [47]. Moreover, AI technology can aid public safety in various ways.

In the area of EMS, AI is able to do a real time injury diagnosis of passengers after a car crash. In a car crash case, data is being transmitted and translated into a medical report in real time, which is in turn being sent automatically to the hospital. In the area of law enforcement AI is linked to video-protection, especially in situations involving crowd movements, abandoned objects, searches of persons of interest, and so on [48]. In addition, through the use of AI crime prevention and prediction is possible. Moreover, an AI-enabled human & object detection and tracking combined with a knowledgebase and behavior analysis could make video surveillance much more effective, and even help prevent crime [48]. To conclude with, AI technology has been by public safety agencies to identify response and mitigate crises and disasters like floods, earthquakes and wildfires. AI and ML algorithms have been also combined and used for severe weather forecasting.

(vi) Data Analytics

The rapid development of data analytics technology has given the chance to public safety agencies to upgrade their decision making in disaster management. In other words data analytics have made it possible to employ advanced techniques to reveal patterns, trends, and associations that enhance situational awareness in emergency scenarios [49]. Emergency response is becoming more and more data-driven. In addition, the use of data analytics can offer a number of benefits to all public safety organizations. Some of them are:

- Storage of Data: Huge volumes of heterogeneous data can be stored through the use of data analytics. With data analytics technologies such as Hadoop, large-sized structured or unstructured datasets can effectively be stored on low-cost commodity hardware [50].
- Real time analysis of Data: During disasters public safety organizations receive large volumes of unstructured data. Data analytics technology has the ability to perform fast analytics with real-time queries which is vital to help decision makers obtain required results for an effective emergency response.
- Cost - effectiveness: Data analytics tools are most commonly open-sourced. Governments all over the world which simply lack the funds can easily access to these tools for free instead of spending large amounts of money for other software.
- One of the main advantages of using data analytics is that it enables data scientists to analyze huge volumes of data involving different data sources that may not be collected using traditional tools [51].

Through the use of data analytics, public safety agencies have the ability to find hidden patterns. In addition, these hidden patterns are extracted for various sources of data from disaster sites.

(vii) eXtended Reality (XR) (umbrella term for AR,VR,MR)

We refer to eXtended Reality (XR) as the umbrella term for other technologies such as Augmented Reality (AR), Virtual Reality (VR) and Mixed Reality (MR) as well as all the future technologies yet to be developed. Furthermore, VR introduces the user to a virtual but interactive environment. In addition, AR has the ability to mix digital content with the psychical world surrounding the user. Moreover, MR is able to blend the real and the virtual word by creating complex environments for the users. These technologies are already used for public safety purposes.

For instance, the healthcare sector is already using AR to bring significant advantages to practitioners who can benefit from digital information projected over real-life images used to prepare operations [52].The next big thing of XR technology is about training first responders in real scenarios. Public safety organizations now aim to make virtual reality simulations for first responders, enabling firefighters, law enforcement officers and others to learn and practice how to best operate and communicate in emergencies [53]. These virtual scenarios could include firefighting in hotels or responding to terrorist attacks for police officers.

(ix) Deep Learning

Deep Learning is one of the techniques based on Computational Intelligence (CI) and has its origin for Artificial Neural Networks (ANNs). ANNs are computational models inspired by neural networks a human brain pocesses. It allows computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction and is able to discover intricate structures from natural data in its raw forms without the needs of sophisticated feature engineering and tuning [54]. Deep Learning can analyze a large amount of complex data (sensing devices, image, video streaming etc.) in smart cities. Researchers in smart cities have applied deep learning in many domains, e.g., traffic prediction, healthcare, air quality prediction and public safety[55].With the use of deep learning and analyzing data extracted from various sources in the city, public safety agencies are able to enhance the security of civilians. In the area of law enforcement, the use of Deep Learning has given the chance to police departments to run face recognition algorithms. It is the process of uniquely verifying (1:1 match) or identifying (1:N match) a person by comparing and analyzing patterns based on the person's facial contours [55]. In addition, face recognition is a powerful tool for law enforcement as it aids crime investigations. Another way of using deep learning for public safety needs is about automatic vehicle detection and recognition. Data is gathered from traffic surveillance cameras situated in city roads. With the use of Deep Learning police officers have the ability to detect and recognize possible black listed or stolen cars almost instantly.

(x) Mobile Edge Computing (MEC)/Fog Computing (FC)

Mobile Edge Computing (MEC) refers to computing at the edge of a network. The edge is similar to a distributed cloud with proximity close to the end user that delivers ultra-low latency, reliability, and scalability [56]. In other words, MEC is in position to enable a wide range of benefits for first responders, including real-time analytics of video surveillance, V2V communications and traffic management. Moreover, through MEC technology first responders such as firefighters and police officers will be able to connect to live surveillance feeds for facial recognition and produce alerts. Furthermore, MEC enables V2V feature. This means vehicles of first responders have the ability to communicate to each other and exchange critical information.

Nowadays, public safety agencies gather data from various sources such as sensors, mobile devices and common people. This is called crowdsourcing. In addition, cloud computing is a technology used by public safety services to analyze this kind of data. In disaster scenarios (natural and man-made) early detection is vital for the perseverance of human lives. In such scenarios crowdsourced data is created and analyzed to a cloud platform. However, analyzing crowdsourced data to the cloud takes time and precaution measures cannot be executed by public safety officers in order to protect civilians. Therefore, fog computing is the new and efficient way to analyze such critical crowdsourced IoT data of disasters [57].

Fog computing is more efficient in analyzing critical data than cloud computing for a number of reasons. Some of them are [58]:

- Low latency.
- Loss of connection is impossible.
- High level of security.
- No bandwidth problems.

Therefore, it is important to mention that cloud computing is more powerful that fog regarding computing capabilities and storage capacity [58].

(xi) Cognitive Radio

Cognitive Radio (CR) is defined as "an intelligent radio that can obtain the knowledge of radio operational environment and established policies and monitor usage patterns and users' needs; to dynamically and autonomously adjust its operational parameters and protocols [59]. In addition, some of the functions CR provides to its users are spectrum mobility and spectrum management. These functions enable the needed flexibility for public safety users during emergencies when current fixed infrastructure is destroyed or partially destroyed. Furthermore, during disasters public safety agencies use a large number of wireless communication technologies. The use of multiple communication technologies and frequency bands allocated for public safety needs leads to network congestion. Existing network infrastructure won't be able to provide stable and efficient communication to public safety users due to their increasing demands.

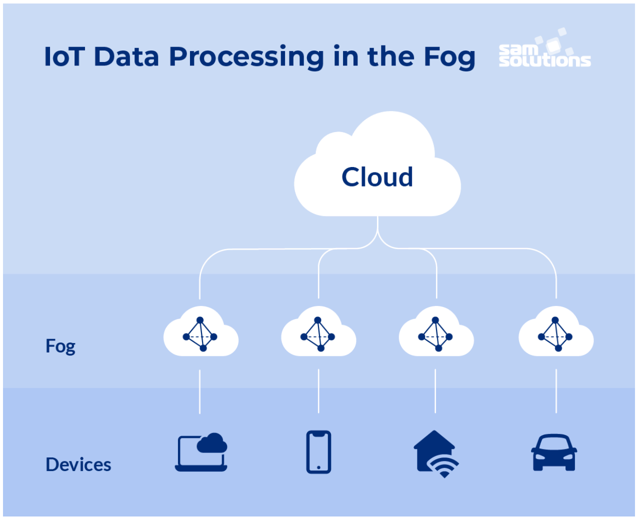

Figure 2.10: Data processing in the Fog [58]

The CR technology is the answer to this problem. With the CR technology, public safety users can use additional spectrum such as TVWS for daily operation [59]. In addition, CR creates additional network capacity for public safety needs providing relief to the existing network infrastructure. In addition, CR technology provides additional flexibility and efficiency for overall spectrum use [60].Moreover, public safety agencies can access licensed spectrum in 700 Mz (band for emergency use)by doing spectrum sharing partnerships with commercial operators, e.g., in areas where public safety wireless network is not available or an effective response to emergency requires more network capacity [60]. CR enabled emergency networks can be used for locating survivors in harsh environments and operate as a stable network platform for devices which use different frequency bands. By this way CR technology gives solution to another big issue which is device interoperability. As we can see in Figure 2.10 in a CR enabled network, CR devices along with the spectrum coordinator respond to the emergency and coordinate with users in the emergency incident area to ensure that first responders can communicate efficiently [62].

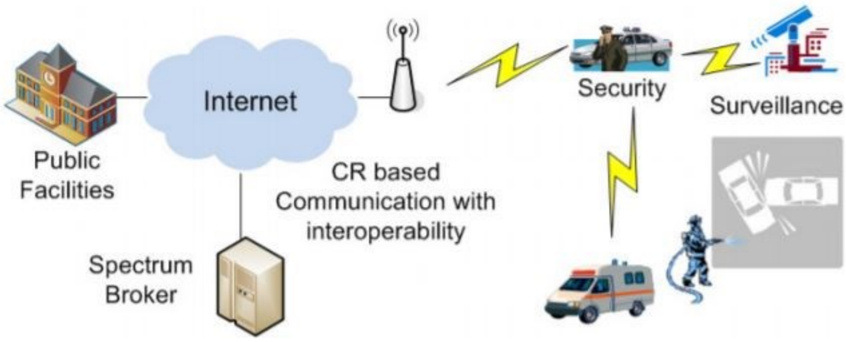

Figure 2.11: CR enabled emergency network [59]

3 Communication Technologies

3.1 Overview of cellular technology for PS

Throughout the years public safety organizations used cellular technologies in order to deliver their services efficiently. In addition, every generation of cellular communication technology used by public safety is categorized by (G). It is worth mentioning that every generation brought a set of new and groundbreaking features to the table for first responders and public safety agencies to use. Furthermore, these new technologies may include new frequency bands, higher data rates or interoperability. Since the establishment of the first generation (1G), we can say that movement from one generation to another takes approximately 10 years [63]. Moreover, the first generation was situated in 1980. 1G was established in the 1979. On the other hand 2G was established in 1991. In addition, third generation brought new revolutionary characteristics such as support for multimedia (video, image) and spectrum. 3G network was developed and deployed in 2002. However, a serious amount in operational disadvantages of (3G) led the governments and public safety organization to the creation of the fourth generation (4G). 4G was introduced in 2009 and supported all IP-switched networks [63]. To conclude with, growth in mobile technology and the rising demands of mobile data services has gone beyond the 4G capabilities. Thus, the need of researching a new generation (5G) to respond with the new status was more than urgent.

3.1.1 Roadmap to 4^{th} Generation - Long Term Evolution

In this Section we will analyze in detail cellular communication technologies up until the 4^{th} generation and their unique features. Figure 3.1 depicts the timeline and summarizes some characteristics of the generations of cellular technologies used by public safety agencies.

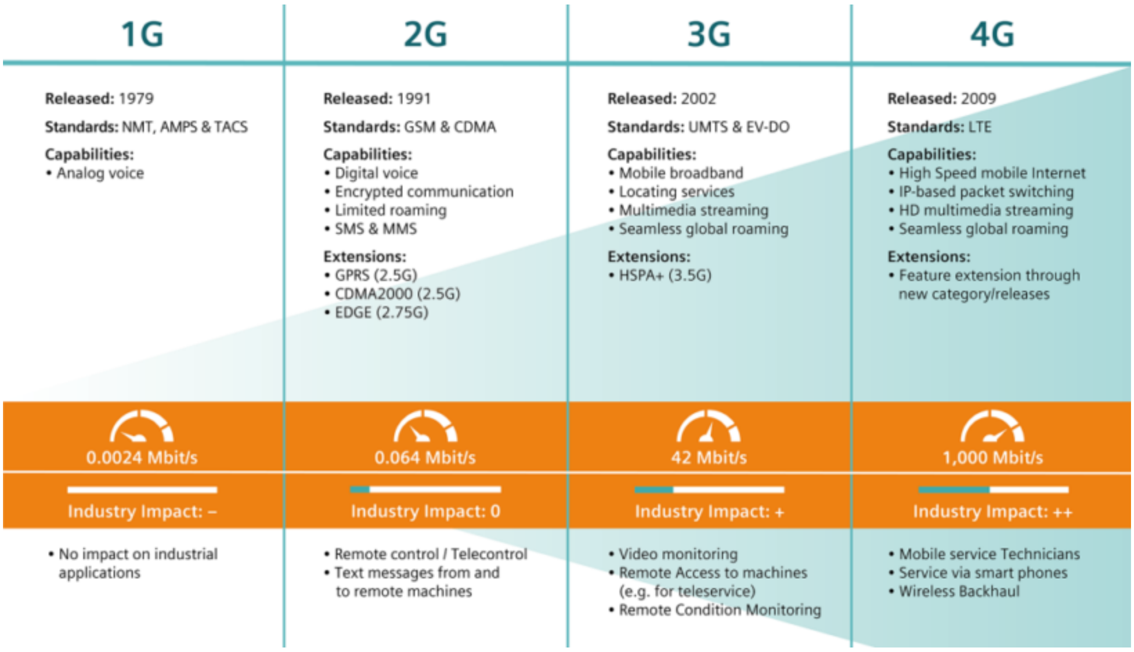

Figure 3.1: Generations of Cellular technology for public safety [68]

(a)First generation (1G)

Starting with the first generation of cellular technology for public safety, devices supported by this current network were all analog. Furthermore, 1G technology brought forward analog cellular networks for use. In addition, these devices mainly operated in the frequency band of 150 MHz.1G introduced the use of multiple cell sites, and the ability to transfer calls from one site to the next as the user travelled between cells during a conversation [64]. However, 1G networks had a number of operational problems that limited their use, which made the need for advancement to the generation urgent.

(b) Second generation (2G)

The main feature introduced by the second generation was the use of digital transmission instead of analog which was used by the first. Passing from analog to digital signal led to mass-adoption by consumers businesses and public safety organizations on a scale never before seen [64]. In addition, 2G was more advanced as it used digital signals for voice transmission that had a speed of 64 kbps [63]. It is also important to mention that this generation also supported an instant text messaging service (SMS) and a multimedia service (MMS). Furthermore, a number of mobile technologies were used by this generation such as GPRS and GSM. Digital signals used by 2G required less battery consumption. Moreover, Digital coding improves the voice clarity and reduces noise in the line [65]. Digital signals produced by 2G are friendly for the environment. To conclude with, 2G upgrade safety of communication with digital encryption which provided secrecy to data and voice calls.

(c) Third generation (3G)

Third generation uses a large variety of wireless communication networks. These networks are the first with broadband technology introduced to the public. In addition, 3G networks are designed for voice communication but also support data-based characteristics such as multimedia and text messages. The widespread use of mobile phones required the need of greater data speeds. 2G generation was incapable of supporting these data speeds so the 3G was established to cover the needs. The main technological difference that distinguishes 3G from 2G technology is the use of packet switching rather than circuit switching for data transmission [65]. 3G increased data transfer capabilities and brought a revolution in the way public safety services or simple consumers communicate. Moreover, increased data transfer capabilities offered new services. 3G networks operate at 2100 MHz and have a bandwidth of 15–20 MHz, thus offering high-speed access to internet services such as video streaming and video chatting [63]. To conclude with, some of the main drawbacks of 3G comparing to the former generation are:

- Higher price due to high adoption rate of 3G from the public.
- Higher power consumption due to high bandwidth transmission.
- Big network overload caused by high bandwidth transmission.

(d) Fourth generation (4G)

Fourth generation is an extension of 3G offering more bandwidth and services. 4G offers fast mobile web access (up to 1 gigabit per second for stationary users) which facilitates gaming services, HD videos and HQ video conferencing. The first two commercially available technologies billed as 4G were the WiMAX standard and the LTE standard, first offered in Scandinavia by TeliaSonera [65]. The adoption of 4G LTE as candidate for public safety communications introduces a unique opportunity to improve the response of PPDR organizations and it will bring high-level applications to first responders [66]. LTE networks include a flexible air interface with low latency making them ideal for public safety use. In addition, another important feature of LTE is the enhanced performance supporting flexible channel bandwidths from 1.4 to 20 MHz in both uplink and downlink directions[66].Some other advantages of 4G comparing to 3G include [67]:

- Shorter round trip delays (RTT) giving more responsive systems
- Improved Quality of Service (QoS)
- Carrier aggregation enabling frequency band combining to make more bandwidth available for users
- Lower implementation costs for public safety operators due to simplified 4G network.

However, the fourth generation includes a number of drawbacks such as the creation of higher bit rates in large cells. Furthermore, another important disadvantage is the issue of different frequency bands limiting the use of similar devices in different continents [66].

3.1.2 Jumping from the 4G to 5G

Differences between 4G and 5G are enormous as we can see in Figure 3.2. More importantly, features such as latency and data rates have upgraded dramatically with the use of 5G. Furthermore, the available spectrum has increased from 3 GHz to 30GHz. Another important feature which was improved is the connection density from 100 thousand connections/km^2 to 1 million connections/km^2. In addition, 5G provides ultra-high reliability comparing to 4G and is ready for the use of IoT technology. 5G could has enormous effects in public safety as it offers the possibility of innovations such as remote surgeries, telemedicine and even remote vital sign monitoring that could save lives [64]. Furthermore, 5G is set to have a massive impact on public safety. Public safety organization with the use of 5G networks will be able to operate security systems for monitoring vast regions in case of emergencies. These security systems will be equipped with millions of sensors which can locate emergency situations, for instance a natural disaster. To conclude with, 5G generation offers higher quality of voice and video calls and faster download and upload speeds comparing to 4G.

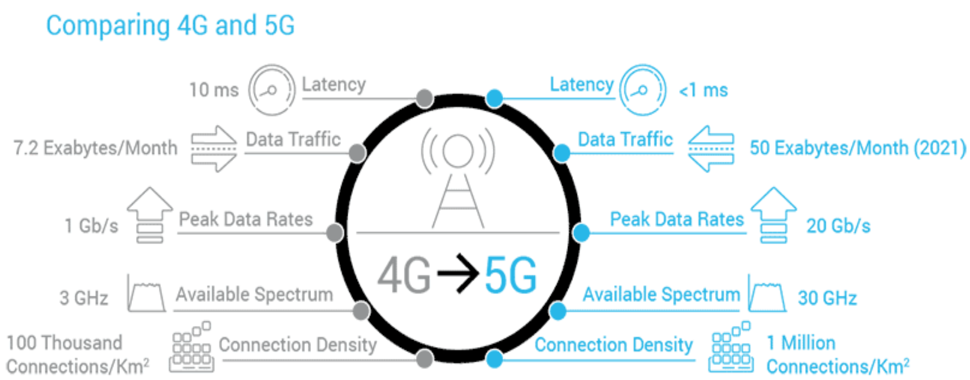

Figure 3.2: Comparison between 4G and 5G [69]

3.1.2.1 5th Generation

5G is the next generation of telecommunication. 5G is gaining vast attention from the research community. 5G overcomes many 4G limitations as it provides high data rates, massive connectivity, ultra-reliability, high spectral efficiency and very low latencies.Moreover,5G is standardized by 3GPP Releases 15-16. In addition, 5G is addressing multiple professional markets apart public safety. Some of them are smart cities, automobile industry and education. Government services could also be highly benefited with the implementation of 5G. In order for 5G to be implemented faster for use several techniques are proposed. One of them is the cooperation between multiple radios in wireless devices. The upcoming 5G systems are envisioned to have the crucial capabilities such as network flexibility, (re)configuration and resilience and therefore, expected to play a key role in improving disaster situation communications [70]. In addition, these capabilities can prove to be more than crucial during emergencies and calamities as they enable faster response and decision making for public safety agencies. Figure 3.3 depicts the key content of 5G. 5G is aiming to implement better from the previous generations in several features [63]:

- Reduction in power consumption
- Reduction in total costs
- Higher data rates
- A high number of concurrent data transmission paths and hand over
- Interactive Multimedia services such as voice calls and video calls.
- Reliability and Security. 5G will provide several new technologies which improve the reliability, availability and security of communications. These include Device-to-Device (D2D) communication, user- and control plane separation by using Software Defined Networking (SDN) and Mobile-Edge Computing (MEC) [67].
- Traffic prioritization. Communication among first responders during emergency incidents must be the top priority of networks instead the communication needs of the public.
- Application aided with AI.

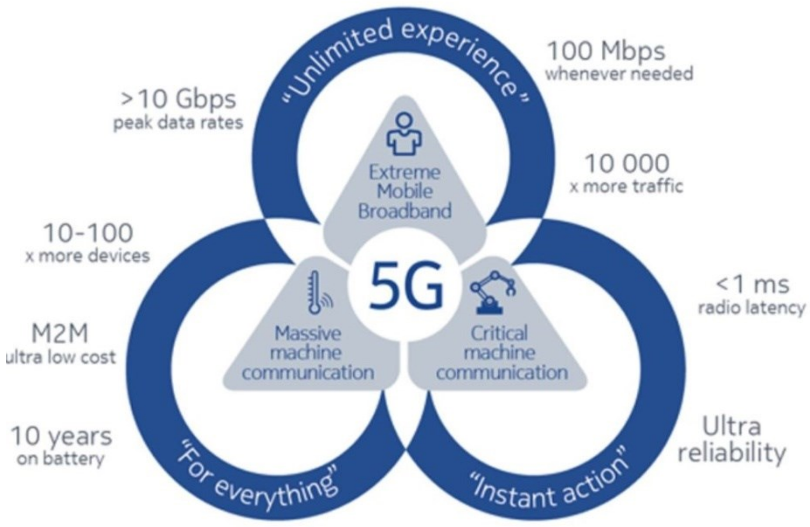

Figure3.3: 5G key content [67]

3.1.2.2 5G's New Radio (NR)

The 5G wireless communication networks will use a new wireless access technology called New Radio (NR) [71]. NR is standardized by 3GPP in the Release 15. In addition, NR has the ability to support a number of wireless requirements and different communication protocols. Wireless networks and communication protocols differ in terms of data rates, coverage and latency.5G NR system will offer a much faster, scalable and efficient network which can support billions of devices and emerging technologies like IoT [72].Moreover, one of the most important advantages of NR is its compatibility. NR is expected to be compatible for the next 10-15 years. It is also worth mentioning that NR is capable of new enhancements in the years to come without interrupting existing networks. Furthermore, NR is able to support various uses cases. Some of these use cases include M2M, industrial use and V2V communication. In addition, Key NR features include ultra-lean transmission, support for low latency, advanced antenna technologies, and spectrum flexibility including operation in high frequency bands, interworking between high and low frequency bands, and dynamic Time-Division Duplex (TDD) [73]. Furthermore, radio interface of NR includes multiple layers. The first layer is the physical layer. Other layers include medium access control and Radio Resource Control (RRC).

As we can see in Figure 3.4, NR includes a diverse spectrum for use, diverse services and diverse deployments. In addition, NR is also highly adaptable to diverse deployments and topologies.

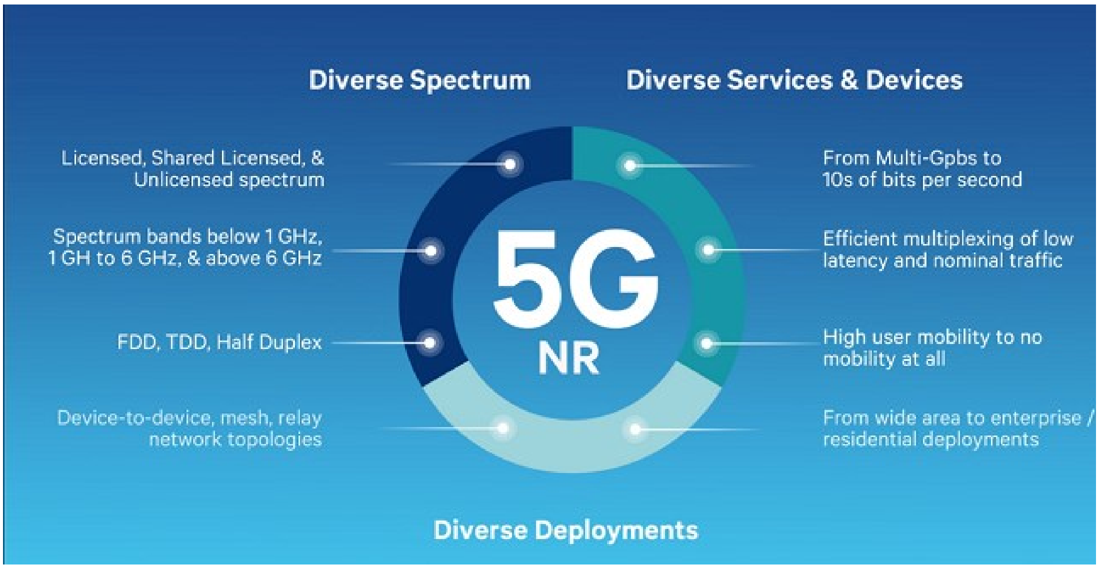

Figure 3.4: 5G New Radio [72]

Furthermore, NR offers scalability to address diverse services use cases. These services may include Massive IoT, Mission-critical control and enhanced mobile broadband. Some of the applications of NR include [73]:

- Healthcare and wearable applications
- Mission critical applications
- Autonomous driving
- Position mapping
- Smart city and security applications
- HD multimedia download and streaming

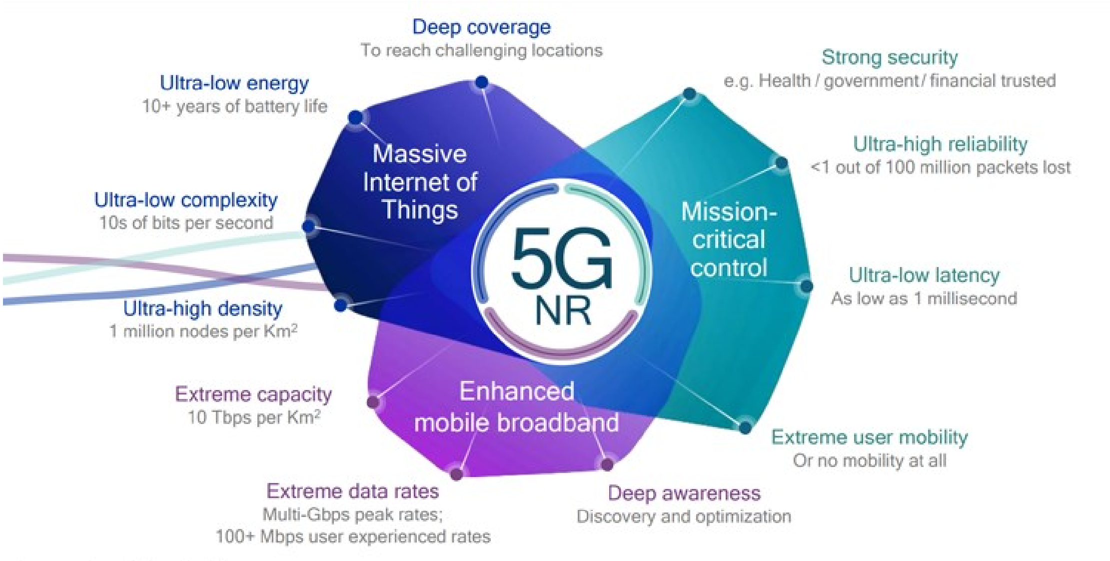

Figure 3.5: Scalability of NR to address diverse services and devices [74]

4 Selected use cases and Scenarios

Before moving on analyzing specific use cases and scenarios it is vital to discuss about the importance of the Disaster Management Cycle (DMC) which involves four stages. Each stage is used by public safety agencies all over the world in order to mitigate or prevent possible calamities that may occur.

4.1 Disaster Management Cycle

In order to understand the exact definition of the DMC we must first define what disaster management is about. Disaster management is defined as 'the integration of all activities required to build, sustain and improve the capabilities to prepare for, respond to, recover from, or mitigate against a disaster [75]. For example, it is the obligation of an emergency medical service to provide care to victims in various disaster scenarios and use cases. Medical services have to cope with difficult situations fast and precise. One bad call could cost lives. Some of the activities related to disaster management are mentioned in the current Chapter.

Disaster management is an important global challenge especially for the case of large-scale disasters that affect many countries and are related to multi-hazards. We will next discuss about the DMC which includes four phases. Two of them (Mitigation and Preparedness) are about risk management and the other two (Response and Recovery/Restoration) are about crisis management (Figure 4.1).

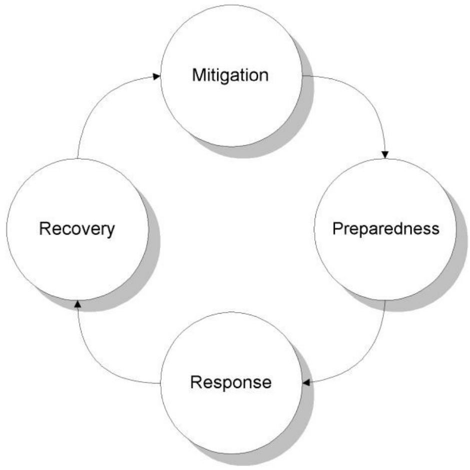

Figure4.1: The four phases of Disaster Management Cycle (DMC) [76]

Mitigation

Mitigation phase includes actions taken to prevent or reduce the cause, impact, and consequences of disasters [76]. Mitigation examples can be found all over the world. From constructing barriers to control flooding, to tying down homes to withstand wind damage. These measures are taken during non-disaster times. To conclude with, mitigation can include development initiatives that enhance physical and social infrastructures [77].

Preparedness

Preparedness phase involves plans and actions conducted in a pre-disaster context [77]. This context includes the response time of public safety agencies right after a calamity strikes. Preparedness phase is slightly different from the mitigation phase which includes more long-term efforts. In addition, preparedness phase includes planning, training, and educational activities for events that cannot be mitigated [76]. Drills can also be conducted by emergency agencies in order to help civilians evacuate disaster sites more safely and quickly. During the preparedness phase public safety officers also inspect buildings, current infrastructure and improve possible vulnerabilities of them in case of a large-scale calamity strikes.

Response

Response phase which occurs in the post-disaster context is linked to the preparedness phase, as it constitutes the efforts carried out during and in the immediate aftermath of a disaster [77]. It is important to remember that businesses and operations do not function 100% during the response phase. During the response stage, public safety agencies implement disaster response plans and conduct search and rescue missions. Evacuation processes are also conducted by public safety agencies.

Recovery (Restoration)

The recovery phase follows the response phase and is aimed at returning normalcy to the communities [77]. Recovery phase may include the restoration of damaged buildings and infrastructure. It is also a vital lesson for public safety operators. During the recovery phase they can learn by the mistakes done during the mitigation phase and try to reduce vulnerability from future disasters.

4.2 Use Cases

We previously referred to DMC and the four stages taking place when a calamity strikes. In the next Section we discuss in detail some of these use cases (man-made disasters, public safety services). Technologies both in communication and application level will be mentioned and discussed too.

4.2.1. Emergency Medical Services (EMS)

(i) Importance of EMS

The first use case we consider is Emergency Medical Services (EMS). EMS is a system of coordinated response and emergency medical care, involving multiple people and agencies [78]. It is also important to mention that EMS is one of the most important health care services as it plays a vital role in saving people's lives and reducing the rate of mortality and morbidity [93]. Figure 4.2 illustrates an EMS system and its complexity. The elements around the circle represent every system activated to respond in a critical situation. Arrows inside the circle indicate the specialty cares that can occur. Finally, the list inside the circle indicates each element which is enabled to support EMS.

These services or systems play a crucial role when it comes down to emergency situations. An emergency situation is called either a natural or a man-made disaster. Moreover, EMS plays a critical role in pre-hospital care during both routine and catastrophic circumstances [94]. The main objective of EMS is to provide instant care to possible victims not only during these events but in any kind of hazard or emergency. In addition, EMS may be involved in search and rescue during earthquake incidents [96]. In order for EMS to be more efficient and resilient activities must be conducted to raise situational awareness and preparedness. In other words, preparedness activities enhance the ability of EMS to deliver care during an event and help mitigate the impact the event will have on a region [95].

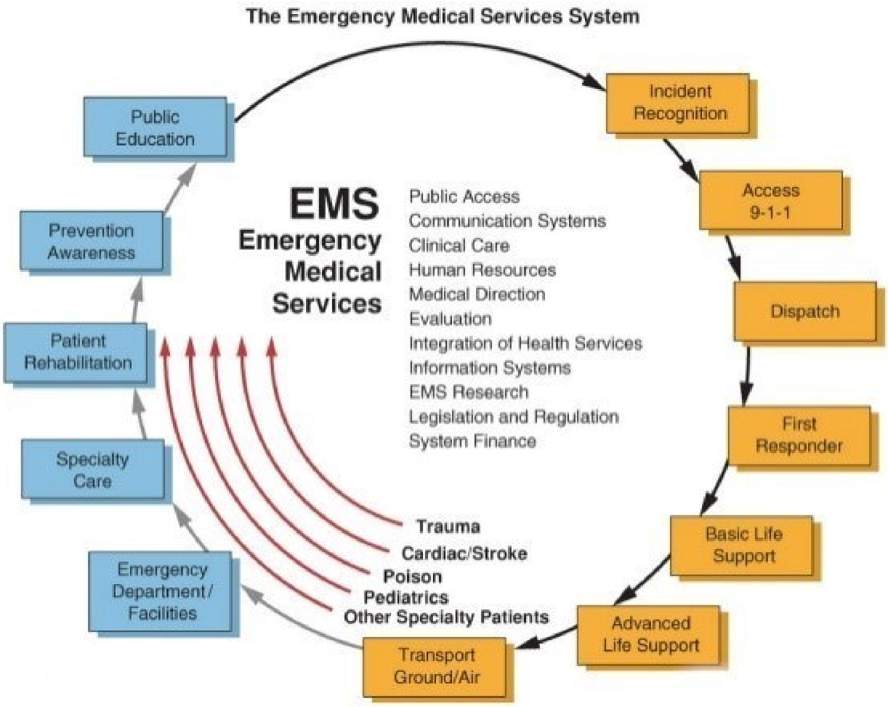

Figure 4.2: Emergency Medical Services [78]

Figure 4.3: The three main pillars of EMS [78]

EMS focuses their operation on three main pillars which are health care, public safety and public health (Figure 4.3). During disaster incidents, response time is a crucial factor, and therefore it is vital that emergency medical services to act quickly and efficiently. Pre-hospital care is another important contribution of EMS especially during catastrophic events and disaster scenarios as mentioned above. Unfortunately, Pre-hospital EMS is effective and efficient under certain circumstances. The performance of Pre-hospitalEMS relies on the existing transportation infrastructure and the medical resources, which are limited and critical [79].

(ii) EMS Technologies

In the previous Section we discussed about the importance of EMS. In order for EMS to be effective, it uses a set of high-end technologies/applications. First responders and medical services use a variety of technologies/applications in order to cooperate and provide care to possible victims during catastrophic events. There are technologies that are already tested and established for healthcare response. On the other hand, there are technologies that could bring a massive change in the way EMS operate but they need further testing in real-time scenarios. The next Section introduces a variety of applications and technologies used by EMS.

Technologies - Applications

a.5G

5G communication technology offers a variety of advantages in various public safety areas. One of them is the area of EMS. Due to these advantages the research community and public safety agencies all over the globe are researching ways to incorporate this technology to their cause. Nonetheless, 5G communication faces many issues. There are numerous challenges and open research yet to be done before 5G technology is implemented in healthcare and EMS. Some issues and challenges of 5G are connectivity in IoT (Internet of Things), interoperability, low power and low-cost communication, big data analytics, security, trust and privacy [81]. Moreover, post-disaster EMS which is currently using wireless communication infrastructure is staying behind in terms of innovation. 5G is the answer to this problem. More specifically, 5G is the revolution of the telecommunication industry, provisions of efficiently handling EMS is expected to be distributed, autonomous, and resilient to the network vulnerabilities due to both manmade and natural disasters [82].

5G is currently serving efficiently and effectively many countries in terms healthcare and EMS. 5G can aid EMS in multiple ways. First of all, 5G is enabling the widespread adoption of IoT for smart healthcare. Secondly, traffic control could be enhanced through the use of5G using vehicles as nodes. In addition, with the use of 5G, public safety is enhanced through surveillance. Finally with the establishment of 5G in ambulances which is the example we will discuss further in detail.

By implementing 5G in ambulances a two-way data communication including audio-visual multimedia flow between ambulances and hospitals [80].This includes in-ambulance video live streaming communication with the hospital. This type of communication allows doctors to give instructions to the ambulance crew about the medical care of the patient when an incident occurs. Doctors can receive the vital signs of the patient such as heart rate, blood pressure and body temperature. Ambulance is connected to 5G network through a micro cell base station (Figure 4.4). Connectivity between the ambulance and the remote-end user (doctor/physician) is achieved by two cases of 5G network eMBB and URLLC.

b. Artificial Intelligence (AI)

Emergency services are required to upgrade with state-of-the-art technology. Artificial Intelligence (AI) is one of the upcoming technologies which can make a great difference in public safety agencies.AI refers to the stimulation of human intelligence in machines that are programmed to think like humans. Devices with the help of AI can become even smarter. Integrating various machine learning algorithms in smart devices helps in making more intelligent predictions [83]. Therefore, these devices in order to be helpful for EMS need to be supported by 5G networks. Smart health-care applications within networks are slowly developing with the help of AI. AI can be established in smart health-care applications used by EMS in the following three ways.

- Via AI algorithms that can be embedded for rapid decision making.
- For low latency services provided by a public safety agency an AI algorithm can perform real time computation.
- AI algorithm can be embedded for the computation and storage of medical data.

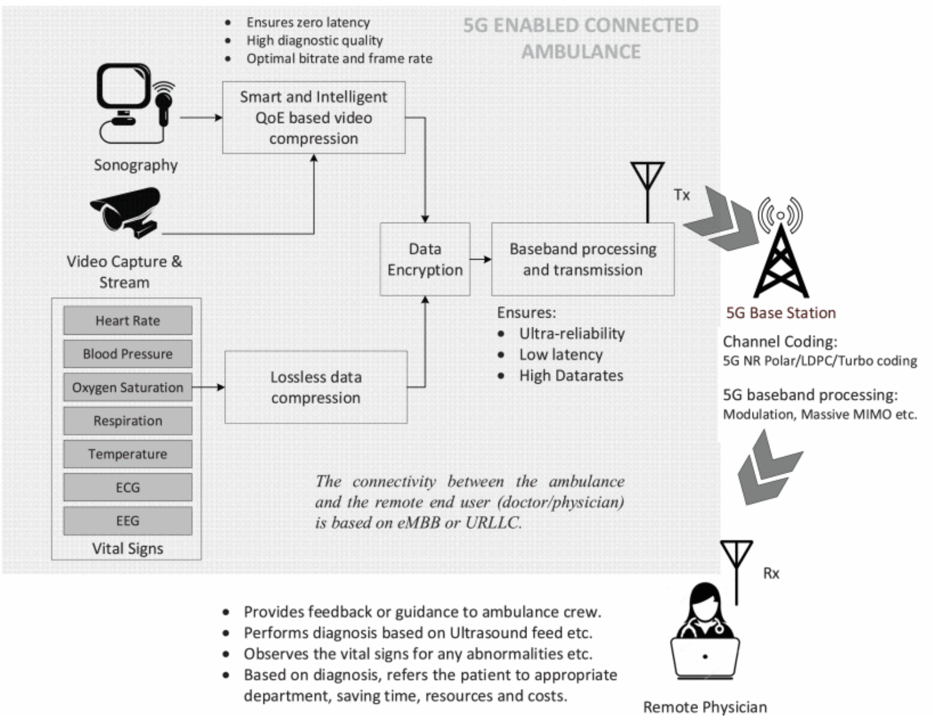

Figure 4.4: 5G enabled connected ambulance [80]

c. Big Data

Big Data is related to large data sets that can be analyzed to reveal patterns. Nowadays Big Data is commonly used in different situations and circumstances providing reliable and effective solutions. The various applications of Big Data analytics include smarter healthcare, multi-channel, finance, log analysis, homeland security and traffic control. In terms of EMS, Big Data can be retrieved from victims located in disaster areas. Analyzing and using these kind of data could prove to be extremely important in terms of minimizing possible casualties. Smart cities use big data to enable crisis response and resiliency.

By gathering and analyzing data, EMS receive real time information about disaster events. With the analysis of Big Data, public safety operators can identify the potential risk, make actions to prevent the risk and finally enable city's resilience [84]. By gathering and monitoring data, EMS disseminates information and gets a better situational awareness about what is happening on ground during a crisis. Therefore we can say that Big Data could play a crucial part in emergency management and could prove to be a powerful tool/technology in the hands of EMS. Big Data and Emergency Management (BDEM), is an emerging research area which springs from fundamentally different intellectual lineages and societal contexts [91]. Figure 4.5 illustrates how big data is gathered during a calamity to help in terms of prevention - response (Learn the Past), Mitigation - Response (Know the Present) and recovery (Future).

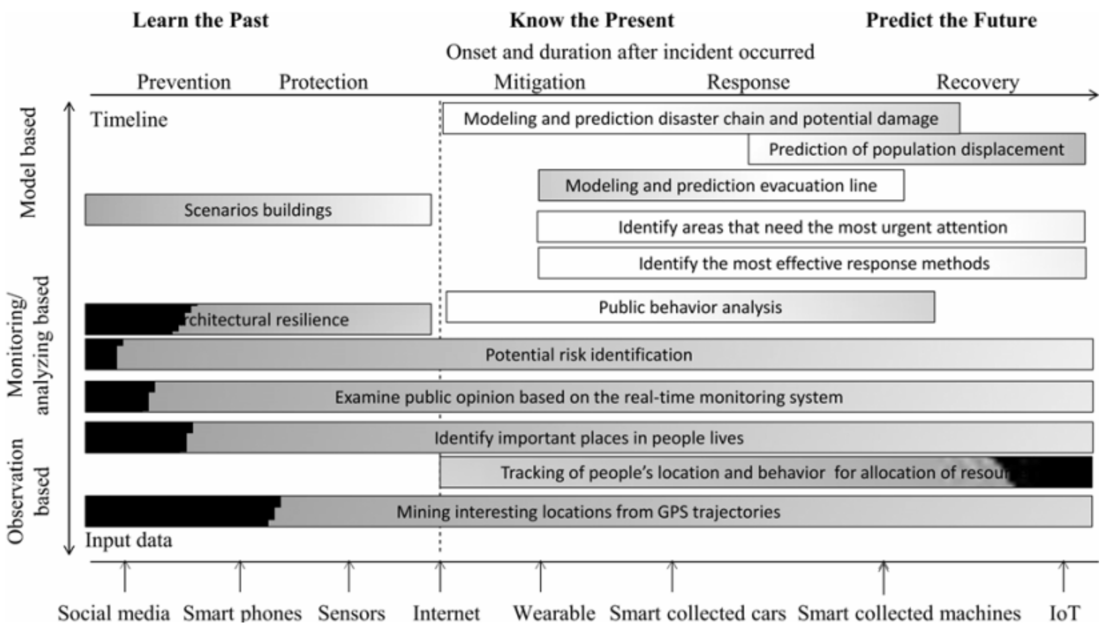

Figure 4.5: Using big data in emergency management during the whole stages [84]

Big data can also be gathered by smart phones and the use of social media applications with the use of crowd sourcing technology. From big data analytics, patterns in the movement of a group of people can be detected, based on their tweets with geo-tag [90]. To conclude with, big data can also be collected by IoT and wearable devices.

d. Cloud Computing

Cloud computing is the delivery of computing services. These services include storage, servers or databases. In terms of EMS, cloud computing can be used to coordinate multiple resources from multiple safety agencies. This is called ubiquitous data accessing. Nowadays, public safety agencies face difficulties in gaining access to critical data simultaneously. Therefore cooperation between them becomes challenging risking human lives. Cloud computing offers a solution to this problem and gives the advantage to each and every medical service to access important data on its own interface.

Different medical services coordinate and cooperate by gaining access simultaneously in a cloud and mobile computing platform which includes medical records. Thus, agencies are making faster and better decisions during disastrous events. Resident health document systems have been built in some districts of cities for residents to store and access their electronic medical records in a cloud computing environment [85]. Public safety operators are able to access data instantly and easily anytime.

e. Intelligent Transportation Systems (ITS)

During disaster events sometimes there is a lack of first responders to provide ambulance services. Moreover, many countries face staffing problems especially in pre-hospital and public safety personnel. A possible solution to this problem is an upcoming technology in transportation of pre-hospital emergency medical services which is the driverless ambulance. It seems that very soon many automotive companies will be focusing on this innovative product. Therefore, autonomous vehicle technologies can make a contribution with the creation of driverless ambulance. However, they are still in the development, testing and approval stages [88].

Despite the fact that a driverless ambulance is an innovative idea which could make a huge difference in the area EMS, there is a vast amount of people openly expressing their concerns referring about the safety and security of this project.

f. UAV (Unmanned Aerial Vehicles)

Unmanned Aerial Vehicles (UAVs) or commonly called as drones, are becoming a more and more popular technology used in search and rescue operations and disaster events. During a calamity some areas are far too risky and dangerous for EMS to approach. The solution to this problem is the use of UAVs. UAVs radically improve the efficiency of EMS in many aspects. First of all, in healthcare possible advantages of using a UAV to transport medicine(s), especially for emergencies, was immediately recognized [92]. Secondly, they can also be sent to a disaster area to gather, analyze and send back to public safety operators valuable data about the size of the calamity. Moreover, UAVs can be combined with infrared cameras to record during nightfall. Finally, as mentioned earlier they are capable of search and rescue operations searching for people reported missing in dangerous areas.

Despite their crucial aid during disaster events UAVs still face a number of challenges and open issues. One challenge is power consumption. Their flights are limited in time due their limited battery. Another important drawback is that although many modern drones are enriched with GIS (Geographic Information System), they still lack the precise sense of location. The drones must have a precise sense of location and understanding of where it needs to go without colliding with moving objects ("sense and avoid") like humans and vehicles [87].

4.2.2. Oil Spill

(i).Oil Spill as a man-made disaster

The second case we consider is about oil spills. As an oil spill we refer to the escape of oil into the sea or other body of water and is considered to be one of the most dangerous calamities existing and sometimes it is nonreversible. There is a number of serious challenges for this disaster to be contained and confronted. Even today the risk of an oil spill is still very high. The main reason is because oil transportation worldwide continues to increase. Number one danger is oil transportation comes from tankers. One small mistake could bring a total catastrophe. In the next Section we will discuss about the environmental effects of oil spills, reasons that cause the calamity and technologies which capable of identifying and containing such disasters.

(ii).Environmental effects - Consequences

Oil spills have enormous impacts both in natural environment and people's lives. Oil spills are environmental disasters that often lead to negative and long-term impacts on the environment [98]. Economic losses of companies and individuals making a living by the sea are huge. Animal life can be severely damaged by the disastrous effects of an oil spill. The first and most obvious effect of an oil spill is the contact of oil with shorelines and organisms that inhabit surface waters, including birds, marine mammals, and reptiles [105]. A potential oil spill can be extremely harsh for nations which base their entire economies in the sea. This is the reason billions of dollars are spent every year for researching and implementing new technologies for response and recovery of such a calamity.

(iii).Reasons that cause the calamity

There are various reasons that can cause oil spills. They are mainly caused by accidents in the ocean, leakage of oil, crude oil or gasoline pipelines [97]. In addition, oil spills can be caused by the human factor itself. Mistakes can be made by individuals being careless or making bad decisions. Furthermore, the breaking down of equipment is a serious factor for causing the disaster. There is a strong possibility that another type of disaster, this time a natural disaster like a hurricane can be the cause of an oil spill. To conclude with, acts of terrorism is one more factor. Oil as a precious liquid can easily be the target of terrorists.

(iv) Identification & detection technologies

In the previous Section we discussed about the disastrous effects of an oil spill. A man-made calamity causes huge problems both in environment and humans. Identification and quick detection of an oil spill disaster is extremely essential. Efficient monitoring and early identification of oil slicks are vital for the corresponding authorities to react expediently, confine the environmental pollution and avoid further damage [99]. Government agencies seek ways to identify and confront faster calamities like an oil spill. A fast response is more than vital. Disaster response and management variables directly influence the severity of an oil spill [106]. Oil can be contained faster making the cleanup process easier. Furthermore, there is a less impact of the operations and less economical damage if it is occurred inside a port. For all these reasons a fast identification (less than 30 min) is important to achieve [103].Public safety services research ways to combine technologies in order to identify and confront an oil spill more efficiently. One specific example of combined technologies will be introduced too in the following Chapter along with other important identification and detection techniques.

(a) Boundary determination and leak detection for oil spill using IoT

When an oil spill disaster occurs, it is important to calculate the full extent of the damage. Determining the bounds of an oil spill can be a very difficult task. The severity of a calamity like this can be measured by setting up nodes on a grid creating a Wireless Sensor Network (WSN) underwater system for surveillance. Nodes are distributed by an underwater robot at specific coordinates. These coordinates are usually determined by the area the calamity covers. These nodes can detect the presence of oil and give back data when a threshold is overtaken. Each high-power node broadcasts a beacon message to the ground level sensor node to indicate its presence in the grid [97]. In the final stage, after all observed data is collected by the nodes, boundary determination of the calamity is calculated.

In addition, IoT technology can be used to detect possible leaks from oil pipelines. Oil spills from pipelines are extremely easy to happen and difficult to detect. These pipelines are usually buried beneath the ground and factors such as rust and breakage could cause an oil spill accident. IoT technology has the ability to collect and process pressure signals, and detects the leakage by using negative pressure wave method to locate the leakage position, it is effective and exact[104]. This way when a blowout or an oil spill accident occursthe negative pressure waves send back signals defining which pipeline presents oil leakage almost instantly.

(b) Identification of oil spill using SAR images and Deep Neural Networks

An extremely reliable way of identifying an oil spill is SAR images. Active microwave sensors like Synthetic Aperture Radar (SAR) capture two-dimensional images [105]. SAR images can operate efficiently even in bad weather conditions. In other words, Imaging radars, like the Real Aperture Radar (RAR) and SAR, are key instruments for oil spill monitoring, because they yield data independent of the time of the day and independent of weather conditions as mentioned previously [107]. SAR images define the oil spills as black spots. Black spots probably related to oil spills can be clearly captured by SAR sensors, yet their discrimination from look-alikes poses a challenging objective [99]. In order for this discrimination to become easier neural networks are used for classification. Neural networks follow three main steps in order to discriminate oil spills from look-alikes via SAR images.

- Detection of dark spots in the SAR image by applying binary segmentation
- Feature extraction from regions
- Yes/No classification as oil spill giving the ground truth.

Figure 4.6 depicts the main SAR image as it is without processing and the same image after the three processing stages.

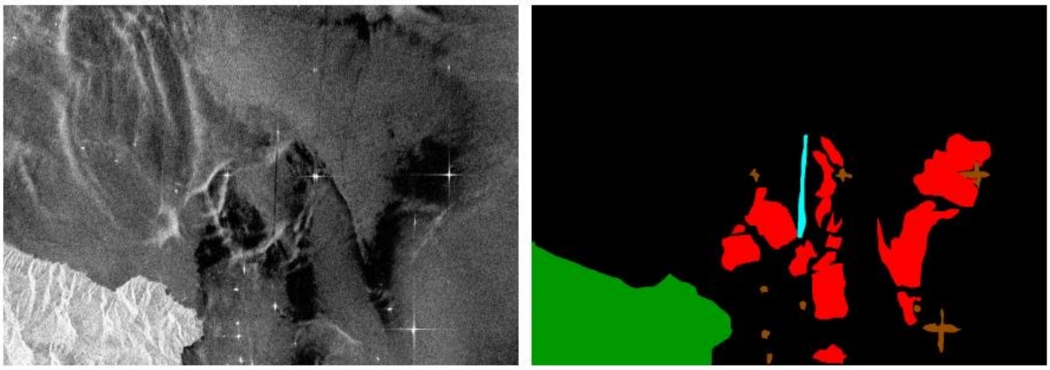

Figure4.6: SAR image before and after processing for identifying an oil spill [99]

(c)Combination of Deep Learning and UAV

As mentioned earlier in this Section, in order to for an oil spill disaster to be identified and detected more than one detection technology can be implemented. The combination of Deep Learning (DL) and UAVs is a reliable solution. UAVs are commonly used by companies to inspect their facilities. With the development of AI, the use of deep learning to process images can enable UAVs to automatically and accurately detect oil spills [101] .UAVs are a cheap solution for quick detection and early warning not only for an oil spill calamity but all kinds of disasters man-made and natural. UAVs are cheaper, smaller, lighter, practical and more user friendly than all other geo-informatics observation equipment [102].

They can provide the public safety agencies high resolution images without demanding large organizations in confined spaces. Figure 4.7 depicts the way UAVs collect images (data sets) used by DL models for oil spill detection. After data is gathered by the UAVs it is sent through a wireless base station to an oil spill detection model for further analysis and finally to an oil control and monitor center for the final classification results.

On the other hand, DL technology through a neural network can be used to process images taken by UAVs directly from the disaster site. A Deep Convolutional Neural Network (DCNN) model is created which separates the data set into two subsets the training and the test set. The separation is done for faster and more efficient results in order to classify a potential oil spill. Before the separation a preprocess method is implemented by adding brightness to images. An oil spill probability is determined by preset thresholds given by the model.

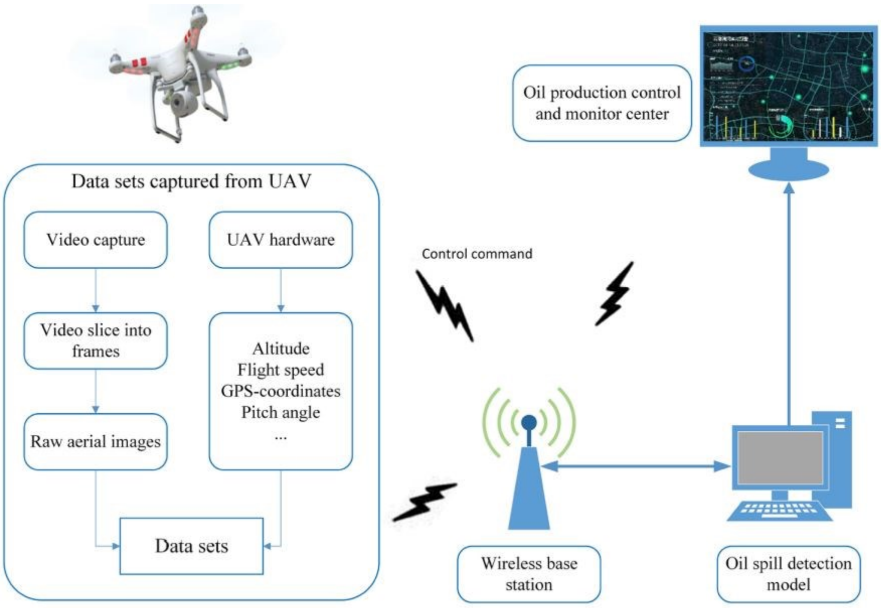

Figure 4.7: Data set acquisition from UAVs [101]

4.2.3. Nuclear disasters

The third use case we consider is nuclear disasters. A nuclear disaster is one of the most devastating man-made disasters. Multiple events can trigger a nuclear emergency. This kind of disaster can be triggered either by an act of war, sabotage or a nuclear accident. More specifically a nuclear disaster can be caused by nuclear atomic bombings or malfunctional nuclear power plants. There have been a number of nuclear disaster incidents throughout the human history. The most serious of them are the SL-1 accident in 1961, the Three Mile Island accident (1979), the Chernobyl disaster (1986) and finally the most recent one the Fukushima daichi nuclear disaster (2011). It is important to mention that the first nuclear horror mankind faced is the nuclear strikes in the cities of Nagasaki and Hiroshima in World War II.

(i)Management of a nuclear disaster

After providing the definition of what exactly a nuclear calamity is, it is important that we point out possible ways to manage it. A nuclear disaster is extremely difficult to handle, many possible factors must be considered by public protection agencies. A nuclear calamity is far more complex than a natural disaster. Public protection agencies have the huge burden to reduce radioactivity. This task requires a set of technical equipment. It is also important to mention that many ministries must cooperate with each other in order to provide the ultimate protection to the people near a nuclear calamity. The human factor is also vital. Individuals should be a part of management. There is growing realization that no public awareness program has materialized so far [108]. Aspects of a nuclear disaster management plan should be known to public for its protection. Some of the aspects are:

1) Nuclear disaster shelters
2) Water supply in radioactive zones
3) Rescue and evacuation plans

(ii)Effects of a nuclear disaster

A nuclear calamity causes countless negative effects both in humanity and the environment. The effects of nuclear disasters on individuals and society can be diverse and long lasting [115]. After a nuclear disaster is caused by a power plant meltdown high levels of radiation are released. Nuclear radiation can fatally damage human DNA. Radiation can also alter the DNA of animals too. Nuclear accidents such as Chernobyl and Fukushima became evident that have socio-economic and psychological impacts on the human factor. Stigmatization of both exposed and evacuated populations following both accidents has strongly contributed to a significant rise in alcoholism, depression, anxiety, bullying and suicides [109].

(iii) Social media as a mean of communication during nuclear disasters

In this Section, we will refer to social media as a communication medium used by public authorities during a nuclear calamity. Social media are mainly used by public protection agencies in order to inform, aid and eventually prepare the people about an upcoming nuclear calamity. Efficient communication is vital for mitigating calamities such as nuclear disasters, as it saves countless human lives.

Mass media take an important role in emergency management during disasters. They are also important for communication with the public in the post-phase of a disaster, in our case a nuclear disaster. Moreover, emerging and evolving digital technologies, such as social media, offer the possibility of improved nuclear emergency communication, as these technologies have the potential for increased information capacity, dependability, and interactivity [115]. Mass media has the ability to increase public awareness and response during emergency situations. Nowadays, social media has led the communication with the public to a whole another level. Social media allow people to exchange information in virtual communities and networks (e.g., Twitter, Facebook, YouTube, etc.)[110]. These platforms instantly provide information to public safety agencies and eventually aid them. Over the past few years, people facing crisis situations have frequently turned to social media to share crucial information and coordinate their actions [117]. In the example of a nuclear incident social media can provide to individuals and public safety agencies with [110]:

- Crisis communication: Information is given instantly to the public. Rapid flow of information.
- Crowdsourcing: Enabling citizens to do a common task in order to preserve their safety.
- Empowering citizen relationships: During hardships such as hazards civilians need to stay together in order to endure.
- Open data: Open platforms where civilians express their opinion. Active citizens are important especially during nuclear disasters. Social media have enabled an explosion of citizen initiatives in the nuclear and radiological field.

(iv)Technologies for Monitoring, Evacuation& Response

In the previous Section we referred to the social media as a mean of communication public agencies use to communicate with civilians when a nuclear accident occurs. In the next Section certain technologies in terms of monitoring, evacuation, response and mitigation in case a nuclear calamity strikes will be discussed in detail.

(a)Monitoring

Monitoring plays a crucial part when it comes to facing upcoming disasters. In the example of a nuclear calamity, monitoring not only gives the opportunity to public safety agencies to form a sufficient response but saves countless lives too. Various activities in a nuclear power plant such as radiation leakage and nuclear fuel recycling demand constant monitoring. When nuclear radiation is leaked to an open environment the atmospheric parameters like temperature, smoke, humidity, sound and carbon monoxide level increase [114]. Many nuclear power plants have implemented the groundbreaking technology of IoT to monitor these parameters in their facilities. They use a wireless sensor network (WSN) with the help of IoT to provide low cost effective environmental radiological monitoring system. The WSN includes nodes which gather all the vital information and reports back to the workstation every time radiation is released from the nuclear power plant.

(b)Evacuation

Evacuation in the post phase of a nuclear calamity could be a serious challenge for public safety authorities. It includes the withdrawal of population from a nuclear disaster site. An evacuation plan raises the awareness of the public in case of an upcoming threat. It also raises preparedness of individuals and companies. Evacuation is an important protective action for mitigating the consequences of a disaster, especially if an evacuation can be carried out in time before the disaster strikes [116]. In order for an evacuation to be successful communication must be solid and efficient before the calamity strikes. Pre-crisis communication is essential in emergency preparedness, which, in turn, is the key to an effective management of nuclear emergencies [112].

More and more people are living nearby nuclear power plants making extremely difficult for public safety agencies to quickly and efficiently evacuate nuclear disaster sites. As we can see in Figure 4.8 more than 3 million people are living in a 30km radius of nuclear power plant. If the evacuation area were increased to a 75 km radius from the NPP, 152 NPPs would need to evacuate more than 1 million people [111]. There is still big uncertainty of governance plans in case a nuclear disaster occurs.

(c)Response

In case a nuclear calamity strikes response must be not only quick to mitigate the possible effects but efficient too. An example of such a response plan proposes to use the architecture of Intelligent Internet of Things (AIoT) (Artificial Intelligence + Internet of Things) to coordinate with ground, surface and aerial and underwater robots, and apply them to disaster response [113]. The main cause of these robots will be to collect environmental big data from the disaster site and report back to the workstations. With the aid of the robots and their reports, public safety agencies have the ability to create efficient disaster response plans extremely quick.

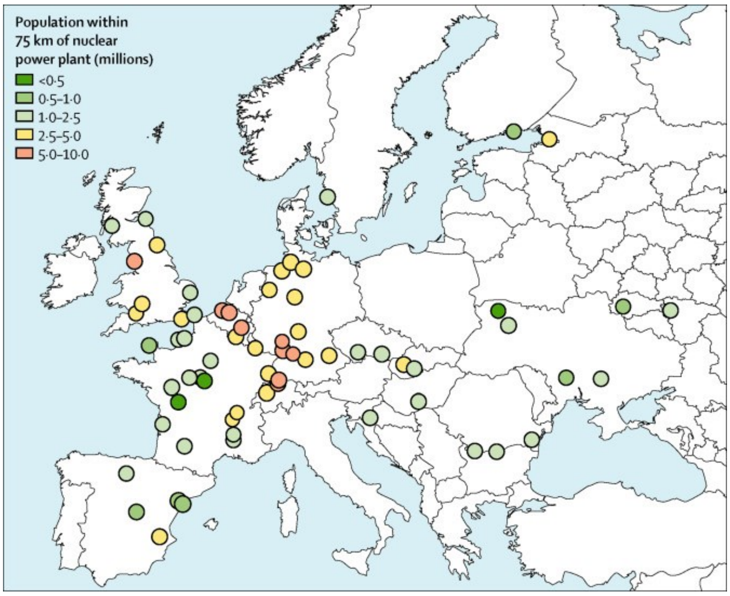

Figure 4.8: Population living within 75 km of nuclear power plants in Europe [111].

4.2.4. Law Enforcement (Crime prevention, crowd control, terrorism)

The fourth use case we consider is law enforcement. The role of Law Enforcement Agencies (LEAs) in each and every country is to fight crime and preserve the law. The biggest challenge LEAs face is how to efficiently and accurately analyzing the increasing volumes of crime data [118]. With the arising use of data LEAs have enabled the ability to collect detailed information of crime data. Technologies used in law enforcement areas like Crime Prevention, Crowd Control and Terrorism will be discussed in detail.

(i)Crime prevention

Crime prevention is one of the most important obligations of LEAs. In order for LEAs to efficient prevent and face upcoming crimes certain technologies are used. Some of them will be discussed in detail below. Upcoming technologies like Machine learning (ML) and Data Mining (DM) provide valuable aid to LEAs. These technologies allow LEAs to analyze large volume of crime data and conduct very important outputs about crime patterns. Thus, one of the challenges faced by the police departments is to minimize threats to society by investigating large volumes of data.

(a) Crime analysis using Data Mining& Machine Learning

Data Mining (DM) plays a crucial role for crime analysis.DM consists of collecting raw data and creating information that can be used to make accurate predictions and applied to real world scenarios [118]. Thus, it has become an upcoming technology in the field of resolving crimes. Analyzing crime data can provide valuable aid to public safety agencies. DM software packages such as the Waikato Environment for Knowledge Analysis (WEKA), the DM software package is used to conduct analysis of data sets by utilizing ML algorithms [119]. Some of these algorithms include:

- Linear Regression
- Additive Regression
- Decision Stump

In order for WEKA to implement these algorithms and output a crime prediction strategy a dataset is required. A crime data set can be used and analyzed by WEKA in order to conduct violent crime patterns. These data sets are provided by public safety agencies.

Another DM technique in order to analyze crime data and conduct valuable output for LEAs is SEMMA which is developed by SAS institute. SEMMA stands for “Sample”, “Explore”, “Modify”, “Model”, “Assess”[127]. Sample stands for various sampling strategies which are used when a data set is too large or complex. Explore stands for visualizing the data. Modify stands for adding extra features to the existing dataset. Model stands for creating predictive models by implying algorithms and creating crime patterns from the given dataset. Finally, Assess stands for the evaluation of the performance of the predictive model.

b. Crime analysis and mapping through online newspapers

Recently, LEAs gained the ability to analyze crimes through implementations of information technologies. It is now possible to define crime trends and patterns by the use of mapping and crime analysis. Information for investigating and analyzing pattern and trends in crimes may come from various sources. The sources may include blogs, news feed and Social Media. One of them is online Newspapers. Online Newspapers refers to the electronic version of the known newspapers. Through online newspapers Text Mining (TM) and Crime Mapping (CM) is possible. Through CM LEAs can identify crime hot spots along with their trends and patterns. In Crime Mapping, we follow the following steps in order to reduce the crime rate are [130]:

- Collection of crime data
- Group data
- Clustering
- Forecasting data.

TM is the process of extracting interesting patterns from very large text database for the purpose of discovering knowledge [128]. TM is also known as (KDT) Knowledge Discovery from Text. It is and IR (Information Retrieval) technique for extracting relevant information wanted from text. The TM methodology of newspapers requires a number of steps. Steps are given below in Figure 4.9.

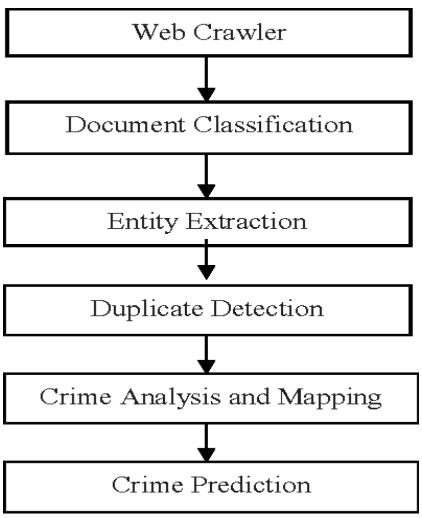

Figure 4.9: *Methodology of TM for crime prediction* [128].

TM for analyzing and creating patterns from online newspapers starts with the web crawler. The web crawler is an internet bot which systematically browses the World Wide Web, typically for the purpose of web indexing [128]. It is used for extracting relevant information. In this case it is searching details-words about crimes. The next step is about document classification. Documents in this case are online newspaper columns and are classified to as crime and non crime based on their content. Next step is about entity extraction. Here the crawler extracts all the valuable information from crime relevant online documents. Entities such as the date and the place of one crime are retrieved. Furthermore, the next step is about duplicate detection. In this step similar documents are found and deleted. This action saves valuable time in order to analyze other unique documents. In the final step crime analysis and mapping is conducted. The results are displayed in graphs and diagrams that include hot spot detection, crime comparison and finally crime pattern visualization. LEAs use this technology to manage the prediction of possible crimes.

c. Crowd Control

Crowd-sourcing enables information to flow quickly and efficiently between emergency management specialists and the public [120]. Tools as Pathfinder and Many Eyes are used for the analysis of the crowd-sourced information. The efficient management of a crowd and the control of huge masses has been one of the top responsibilities of law enforcement officers. A large number of people can be gathered in one place for different purposes and reasons. A crowd may be politically motivated with their own agenda at a political event or supporting their own sport team with heightened emotion at a sporting event [126]. There is a strong possibility one crowd turn violent both to other people and law enforcement officers. It these kinds of behavior LEAs need to counter.

(ii) Terrorism

Terrorism is a crucial problem LEAs face. Terrorist attacks are becoming more and more frequent especially in rapidly developing countries. In order for LEAs to efficiently increase their response in such incidents they use a set of technologies. Some of them include the use of social media, Artificial Intelligence (AI), and unmanned vehicles (ground and aerial).

(a) Unmanned vehicles (ground & aerial)

Nowadays, LEAs use all the possible technologies in order to act quickly and efficiently. One such technology is the use of unmanned vehicles, aerial and ground. An Unmanned Ground Vehicle (UGV) is a vehicle that operates while in contact with the ground (Figure 4.10). An Unmanned Aerial Vehicle (UAV) (Figure 4.11), commonly known as a drone is an aircraft without a human pilot on board [121].

Figure 4.10: The Unmanned Ground Vehicle (UGV) [121]

Figure 4.11: The Unmanned Aerial Vehicle (UAV) [122]

Robotic technology has made a huge difference in disaster response, preparedness and relief. In case of a bio-terrorist attack they can deliver face masks and antidotes to victims. UAVs can also fly in dangerous zones and diffuse bombs planted by terrorists. Robotic technology can be extremely valuable in an active shooter situation. They can provide the swat teams and public safety operators with the shooter's location and movements. In addition, an unmanned aircraft could likely have collected vital intelligence to aid LEAs in more accurately assessing the nature of the threat presented by the shooter [122]. In other words UAVs have a huge contribution in minimizing human casualties.

Furthermore, they even have the ability to create self contained communication networks when the current infrastructure is damaged. In other words they are the eyes and ears of public safety authorities in dangerous times. Drones are systematically used by public safety agencies for search and rescue operations.

(b)Social media

Social media play a crucial part in people's lives. As cybercrime and cyber terrorism threats increase, so does the requirement to consider the potential application of social media as a vital aspect of any cyber defense strategy [120]. With the right use of social media platforms

LEAs possess a powerful tool capable of aiding them in very difficult situations. LEAs can use the social media platforms in critical situations to communicate with the public. Social media platforms depend on civilian engagement too. The more civilians create content the more data LEAs have in their disposal to use. Nevertheless, data must pass through certain stages in order to be used by LEAs. Figure 4.12 shows all the stages content passes through from the moment of its creation to the stage LEAs use it to extract valuable information. This way LEAs fully exploit the use of social media as a communication method.

Twitter is used by LEAs as a crisis communication tool. LEAs use a large variety of social media platforms to share information about an incident with the public. As an incident we refer to crimes, traffic road conditions and other breaking news including a terrorist attack. LEAs also use other kinds of social media platforms such as Facebook and YouTube. Nevertheless, twitter became the number one tool for communication with the public due to its effectiveness. It is very timely, you can update very quickly if we have something, we can send it out immediately [125]. Figure 4.13 shows all the current social media platforms LEAs use to provide the public with breaking news.

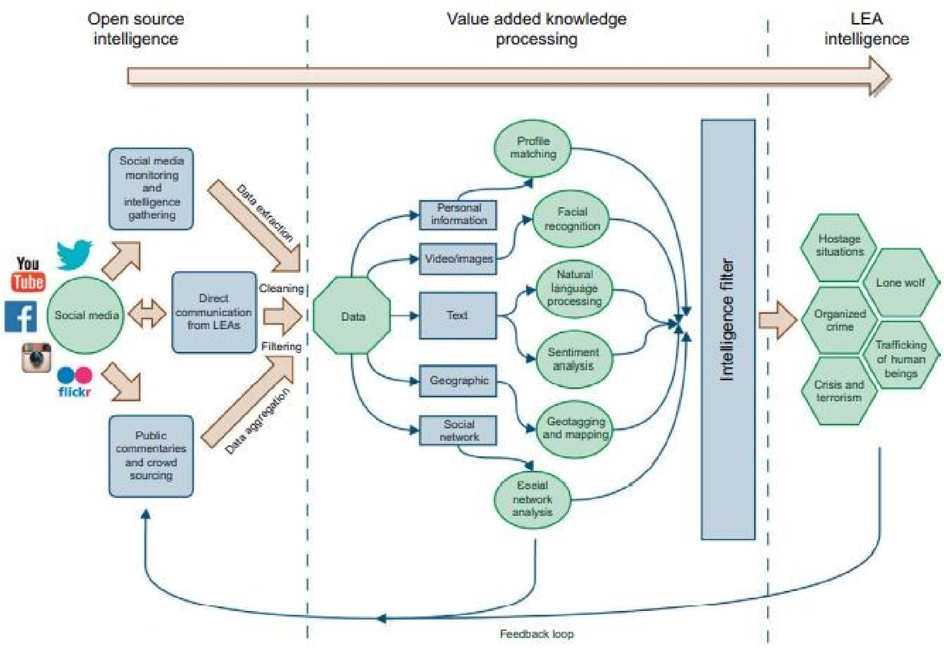

Figure 4.12: From social media to LEA intelligence [120]

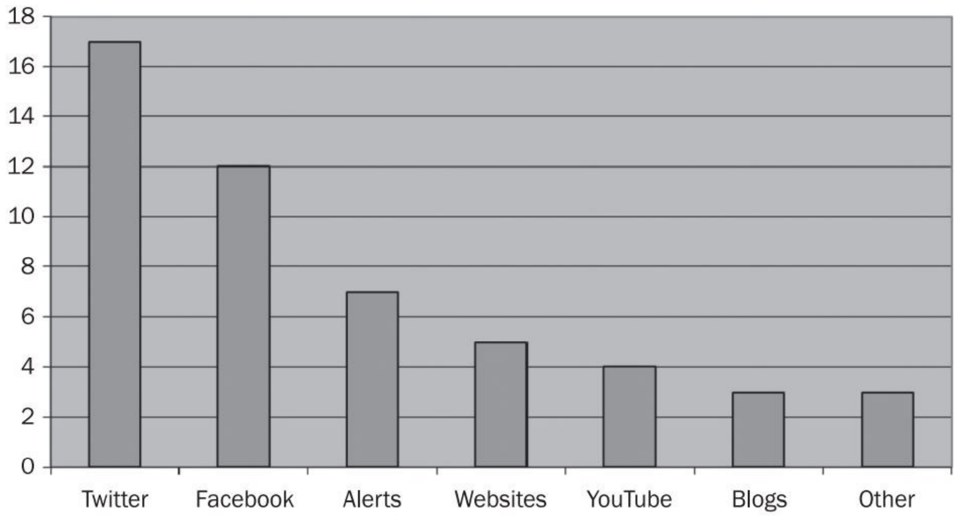

Figure 4.13: LEAs use of communication platforms [125]

(c) Monitoring Terrorist attacks through the use of Social Media

Social media platforms such as Twitter can be used in critical situations by LEAs. One such critical situation is a terrorist attack. Twitter is often used by terrorists to communicate and disseminate their activities. User accounts are extensively analyzed by LEAs in order to counter terrorist actions. LEAs are interested in tracking and flagging terrorist-related activities in social media networks [124]. Tracking terrorist activity in one of the most used social media platforms (Twitter) in the world could prove to be an extremely difficult task. In order to overcome this hardship LEAs use crawlers which search for specific keywords given by the officers. A crawler is a bot that systematically browses the World Wide Web (WWW) in our case twitter and searches for specific content. This crawler searches for the keywords in an extensive amount of tweets for any terrorist activity. Data (tweets) are randomly chosen. Systems with crawlers are currently made by open source tools and extract useful data with the use of R language. The visualization of data can be developed using simple web technologies like JavaScript, HTML5 and CSS.

(d) Artificial Intelligence (AI)

LEAs in order to ensure the safety of civilians in case of critical situation are using all the possible upcoming technologies which can make a difference. One of them is AI and the use of Deep Neural Networks (DNNs). Technology is a powerful ally. The advances of information and communication technologies significantly eased the access to critical and tactical information which can be acquired from various sensors and sources, e.g., wide networks, surveillance cameras and UAVs [123]. Manual analysis of this information is no longer a viable solution. AI gives the opportunity to LEAs to analyze this enormous amount of information and extract strategic knowledge.AI is becoming common among LEAs. Typical applications include suspect profiling (e.g., on social media), traffic control (automated license plate detection and vehicle identification), analyzing dark web money flows, child pornography detection and anomaly detection in surveillance footage of public spaces [129].

In addition, with the help of AI and the analysis of the visual data LEAs can detect strange behaviors (Crowd Behavior Analysis), strange objects bomb-alike (object identification), Lip reading and psychological signals analysis (Body movement). Each and every one of them could be proven to be a very crucial factor in a terrorist attack incident.

4.2.5. Traffic/Transportation Safety (Roads, Air, Trains)

The fifth use case we consider is traffic/transportation safety, one of the biggest challenges public safety agencies have to face. The vast amount of passengers using the public means of transportation urges the safety upgrade of them as soon as possible. There is of course a large variety of upcoming technologies and communication technologies which can aid towards that big step. Some of them will be discussed further in detail below.

(i) Road traffic safety

In the area of traffic safety in roads there are several communication and other technologies aiming to enhance vehicular safety and minimize human casualties.

(a)V2V (Vehicle to Vehicle) communication for traffic safety

Vehicle to Vehicle (V2V) technologies for traffic safety is a look in the future. Automotive industry has been searching ways to reduce the number of human lives caused in the road and reduce traffic congestion. V2V technology is one of the communication technologies capable of resolving this matter. V2V and Vehicle to Infrastructure (V2I) communication are two proposed technological innovations which can change current transportation [132]. V2V is one upcoming communication technologies for vehicular safety.V2V communication enables vehicles to wirelessly exchange information about their speed, location, and heading [131].

In V2V communications, vehicles with V2V software can broadcast and receive directional messages including the proximity of other vehicles. These way road accidents are dramatically reduced. According to NHTSA (National Highway Traffic Safety Administration) 615.000 motor vehicle crashes could be prevented if V2V was used by vehicles nowadays. V2V technology can be implemented in all kinds of vehicles from tracks and buses to motorcycles. It is also important that V2V communication is not only about road traffic safety but preserving the environment too. In addition to their safety applications, V2V and V2I communications can potentially contribute towards reducing fuel consumption and emissions[133]. To conclude with, one of the most important aspects when V2V communication is regarded as a sensor system is the real time ability [134].

(b)Real Time edge analytics and 5G

In order to increase traffic control and safety, certain technologies were introduced to LEAs. Two of them are Real time edge analytics and 5G. Traffic control systems can use these two technologies to minimize the risk of car crashes and human casualties particularly pedestrians. One such system is called InTraSafEd5G which combines real time edge analytics and 5G. It is a system for detecting pedestrians and cyclists in drivers' blind spots at critical traffic intersections and reporting their presence to drivers [135]. Detection of pedestrians or other cars nearby are taken by applying an object detection algorithm on video from edge devices attached on traffic lights. Detection results are delivered to the drivers (using real time low latency 5G communication) to their smart phones providing them with critical situation early warnings for objects to their path.

(ii) Traffic safety for aviation

In the area of traffic safety and aviation there is a number of communication technologies and technologies aiming to enhance safety and minimize the risk of airplane collision. Two of them are ML and the SANDRA project.

Figure 4.14: Vehicles transmit and receive messages from other vehicles (V2V) [131]

(a) Machine Learning for future aviation communications

ML seems to have great potential for upcoming technology for aeronautical communication systems. It is a tool for cognitive radio networks. Cognitive Radio (CR) is an intelligent, adaptive radio network technology in which channel measurements and spectrum sensing are used to automatically detect available channels in a section of wireless spectrum [136]. Applications as CR can be used in aeronautical communication systems. They can help airplanes share resources more efficiently and increase their reliability in safety.

(b). Sandra Project

Air transportation is expected to at least double by 2050. Coping with these needs and the resulting overcrowded sky requires top-notch communication technologies [137]. While the aviation companies provide internet to the customers, pilots have to work with outdated communication equipment such as analogue voice communication causing delayed reaction to upcoming serious incidents. The need to digitalize communication of aviation is greater than ever. A digitalized communication will enhance safety of the passengers dramatically. SANDRA a project from SESAR as a European sky initiative is set to provide to aviation companies increased data traffic and better cabin and passenger communication systems. SANDRA consortium has taken radical approach. It has as its main goal to revolutionize in-flight communications and leads the pilots to the next level of aviation communication. SANDRA project is a single system based on Internet Protocol technology, it is capable of transmitting data through multiple data links, directly to the ground and via satellite, digitally and at high speed, providing communication services for all aircraft needs [137].

(iii) Traffic safety for railways

In the area of traffic safety in railways there are a number of communication and other technologies aiming to enhance safety and minimize human casualties. Some of them are:

(a)DSRC-Enabled Train Safety Communication

DSRC (Dedicated Short-Range Communication) has as one its main goal to implement at unmanned railway crossings. Every year throughout the world there is a number of collisions of trains with vehicles at unmanned railway crossings. It is a very dangerous phenomenon which costs lives of civilians. DSRC has been the main protocol for V2V and V2I communications, and a key technology enabler for Intelligent Transportation Systems (ITSs). One of its applications is early warning. In this case a warning for a collision with a vehicle. DSRC as a wireless communication technology enables vehicles to communicate with each other and other road users directly, without involving cellular or other infrastructure. Each vehicle sends 10 times per second its location, heading and speed in a secure and anonymous manner [139].

(b)Radio communication for Communications-Based Train Control (CBTC)

With the European rail market increasing, railways need to be upgraded with every possible way. A modern communication-based signaling system is required and installed. Communications-Based Train Control (CBTC) is a modern communication-based system that uses radio communication to transfer timely and accurate train control information [140]. It is the main choice of mass transit railway operators. CBTC is modern signaling communication system transferring the data of the trains much faster than the previous radio communication infrastructure. It includes high resolution and provides real time data of trains. With this communication method safety is increased as every train knows the exact location of other trains avoiding the risk of collision. It also reduces the risk of traffic and possible in case of two trains travel in the same railway. CBTC is the first choice of railway operators for mass-transit operations today with currently over one hundred CBTC systems installed worldwide [140].

(iv) Sea traffic safety

(a) Artificial Intelligence (AI) for ship collision avoidance

With the seas congesting more and more with ships and vessels the danger of an upcoming collision is greater than ever. Collision may happen by many factors. One of them is a simple human mistake. It has been estimated that human error is responsible for anywhere between 75% and 96% of all marine accidents [141]. AI could give the answer to such dramatic incidents. With the help of AI and Big data Fujitsu Limited managed to construct a risk calculation model for ship collision. Using risk values calculated by Fujitsu's technologies, operators can proactively detect vessels at risk and prioritize them [141]. This will help in preventive planning while offering accurate information to vessels. The main advantage is that AI can gather and analyze data in real time fast and accurate. In our case, gathering the location of other vessels and their proximity. This risk calculation model could be a powerful tool in the hands of maritime industry and their struggle to minimize the cost of human lives from ship collisions. In Figure 4.15 we can observe a screen image from the Fujitsu collision risk calculation model.

Figure 4.15:Screen image of fujitsu's risk collision model [142].

4.2.6. Recreational (Stadiums - Arenas, Theme Parks) Safety

The sixth use case we consider is recreational safety. Recreational safety refers to safety pertaining to leisure or risk-taking activities [143]. Every activity which includes a vast number of civilians or spectators (sporting event) must be followed by precautionary public safety protocols. Recreational Safety can be found in many aspects. Some typical examples are stadiums - arenas and theme parks. In this Section we will discuss about certain technologies and communication technologies used by public authorities and organizations to enhance public safety in these cases. We will also discuss about communication technologies also used by public safety operators.

(i) Stadiums - arenas

The IoT technology which refers to "all things are connected" sets the foundation of an intelligent stadium-arena. It can be a groundbreaking and revolutionary technology for the operation of a stadium in terms of safety and communication between public safety operators.

(*a)IoT (Internet of Things) for stadiums-arenas*

IoT can be combined with other groundbreaking technologies such as RFID, sensor networks, remote sensing, M2M communication network, the Internet, LAN, and cloud computing to introduce us the smart stadiums - arenas. These technologies increase the efficiency and safety of a stadium. An intelligent stadium is one of the important signs of modern sports venues, stadiums are automation, digital and information development reflects the intelligent stadium, not a unified definition [144].

Nowadays, communication among security employees in stadiums - arenas and public safety officers is the number one priority, especially when it comes down to emergency situations.

Figure 4.16: Devices in IoT [144]

Communication methods must be efficient and steady. For these reasons an intelligent stadium must include a smart communication system. This system increases the communication capability. This system also achieves all kinds of information flow in the internal and external transmission network based on communication between inside and outside the construction of intelligent high-speed processing various images, text, voice and data, information processing and information to meet user needs [144].

The use of IoT which sees people as "objects" gathering data and feedback from them enhances the operational efficiency of the intelligent security system of a stadium - arena. IoT gives the opportunity of high-speed processing of real data taken from the spectators via the LAN network, increasing the ability of preventing disastrous situations like fire and earthquake or even a terrorist incident.

b. UAVs for Stadiums-Arenas

Another important factor capable of enhancing and upgrading communication of stadiums both in normal and critical situations are UAVs or commonly known as drones. UAVs can play a crucial role when comes to communication in sports events. Stadiums - arenas with the use of UAVs can increase network connectivity using the existing infrastructure. This is called UAV-aided communication. UAV-aided communication is an emerging topic in the field of next generation networks [145]. This technology is said to be the next big thing of public safety networks. During sports events with massive number of spectators, UAV-aided communication can enhance the efficiency of communication. UAV aerial BSs can play an important role in improving the network capacity and coverage in crowded areas such as stadiums by offloading the traffic from the cellular infrastructure with minimal network planning [145]. UAVs can also serve as GSM base stations during sports events, not only in normal condition but in critical situations too especially when the current infrastructure is damage. By implementing the GSM technology and they can provide network coverage to users within their vicinity. They can also improve wireless throughput during temporary events such as football games in large stadiums [146].

(ii)Theme parks

Nowadays, amusement park operators are seeking ways to make to manage their premises more efficiently. Their main goal is to provide visitor with a safe environment especially when a critical situation arrives. There is a large number of emerging security technologies and communication technologies that can be implemented successfully in theme parks. Some of them will be discussed further in detail above.

(a)IoT (Internet of Things) for theme parks

IoT technology is said to be the next big thing as it comes to the operation of theme parks. It is said that will transform the experience of visitors. Norton, the security specialists, estimate 11.6 billion devices will communicate with one another over the internet by the end of next year (2021)[149]. The level of security is more efficient once internet connected devices communicate with each other. Real-time communication of these devices is extremely helpful for security employees of the park. IoT technology combined with AI gather a large variety of data of implemented devices throughout the park area and make autonomous decisions without human aid.

Figure 4.17: Connected devices via IoT [149]

Furthermore, IoT technologies aid the theme park industry with multiple ways upgrading security of the visitors dramatically. With the help of IoT maintenance of the theme park rides can be done quicker and smarter. Thus, IoT sensors embedded in theme park rides can collect and transmit a stream of valuable data pertaining to the ride's performance, enabling managers, technicians and engineers to gain unparalleled insight into when the ride needs checking, repairing or upgrading [150]. Other ways IoT technology could contribute in the area of theme parks are proximity marketing and intelligent ticketing. Proximity marketing is done by setting up beacons inside the theme park area. These beacons send signals to the all the visitors smart phones guiding them to particular rides and events. Intelligent ticketing is an IoT technology used by Disney. Disney is one of the biggest brands in the field of theme parks. Disney used IoT technology by implementing into the visitors wristbands. These wearable wristbands, used in conjunction with RFID tags and radio frequency technology throughout Disney's parks, act as a substitute for paper tickets and grant the wearer admission to rides and fast-track queues based on the account information associated with the device [150]. In addition, visitors can use these wristbands to make payments in restaurants and shops located inside the theme park.

There are serious circumstances where implemented IoT technology in theme parks can prove to be extremely helpful and valuable. One of them is missing child scenario in large areas like stadiums and theme parks. A localization framework implemented in the current infrastructure of a theme park is recommended. This framework uses the RSSI localization solution. RSSI is a technique that finds the distance between the transmitter and the receiver by measuring the signal strength on the receiver [151]. With RSSI, IoT localization framework staff of the theme will be able to find out the location of a missing person. Parents and children will wear a smart band with BLE technology. Bluetooth Low Energy (BLE)can work combined with the beacons implemented inside the theme park area and can utilized by multiple devices such as smart phones.

When visitors receive wristbands download an application and in case of a missing child scenario pushes the alarm button to inform the theme park security. The location of the child is calculated by the passing of the worn wristband from each beacon. Beacons are used like nodes in this current situation to calculate the exact position. These wrist bands also include RFID technology. Currently, Radio Frequency Identification (RFID) systems are used in modern theme parks to locate lost visitors [148]. Every wrist band is embedded with active RFID tag. When the visitor is in the coverage area of each reader, the reader senses its presence and sends its location to a server [148].

(b)Push To Talk communication technology

A traditional communication technology used in theme parks by the staff in order to communicate is PTT (Push -To Talk). This way of communication can prove to be extremely helpful in serious situations like a fire incident. PTT provides instant communication among the staff of a theme park. Using PTT for theme parks and large-scale amusement parks allows you to communicate with specific departments that work within your organization such as maintenance and security [152]. A very helpful feature of PTT communication in a theme park is the panic button. It allows the staff of the theme park to send a specific SOS message for a large variety of emergencies such as accidents fires and calls for security.

4.3 Natural Disasters

After analyzing various use cases of man-made disasters it is important to discuss about the other big category of disasters. This of course refers to natural disasters. In the last twenty years extreme weather events tend to be more severe due to the phenomenon of climate change. Figure 4.18 illustrates a large number of natural disasters that may take place. Each natural disaster can be defined as any event with an environmental cause or process that negatively impacts humans.

Natural hazards are naturally occurring physical phenomena caused either by rapid or slow onset events which can be geophysical (earthquakes, landslides, tsunamis and volcanic activity), hydrological (avalanches and floods), climatological (extremetemperatures, drought and wildfires), meteorological (cyclones and storms/wave surges) or biological (disease epidemics and insect/animal plagues) [156]. Every natural disaster has its own level of severity and they are highly unpredictable. Some of them are extremely rare to happen and some of them occur more often in specific geographic locations.

We can classify natural disasters into four categories. Atmospheric, Terrestrial, Aquatic and Biological. In Table 4.1 we can see the full extent of these categories with specific examples in each and every one of them.

Figure 4.18: Typical examples of natural disasters [153]

Classification of Natural Disasters			
Atmospheric	***Terrestrial***	***Aquatic***	***Biological***
Blizzards Thunderstorms Lightning Tornadoes Tropical Cyclone Drought Hailstorm Frost. Heat Wave or Loo, Cold Waves etc.	Earthquakes Volcanic Eruptions Landslides Avalanches Subsidence Soil Erosion	Floods Tidal Waves Ocean Currents Storm Surge Tsunami	Plants and Animals as colonizers (Locusts, etc.). Insects infestation - fungal, bacterial and viral diseases such as bird flu, dengue, etc.

Table 4.1.: Classification of Natural Disasters [157]

Not all natural disasters are deadly. Some of them record a worrying number of human casualties. According to USnews floods, earthquakes and tsunamis are among the deadliest natural disasters worldwide for the year 2018 [154]. Specifically in USA, floods record the biggest number of human casualties than all the natural disasters together. In case of a flood hospitals and public safety authorities must be alerted and ready to medically treat people. Floods cause a number of injuries to people. Some of these injuries need instant medical attention. Hypothermia, trauma from falling debris, and lacerations are just a few of the injuries a hospital will encounter during a flood [155]. We can witness the ferocity of a flood situation in Figure 4.19.

Figure 4.19: A flood situation in USA [155]

5 Challenges/Open Issues

Technologies and applications, which public safety agencies utilize,actually aim to assist first responders to provide more accurate care to possible victims. Nevertheless, technologies and applications of used emergency operations and public safety agencies face also a number of challenges. Some of them are:

5.1 Interoperability

PSNs used by first responders face a variety of challenges. One of them is interoperability. In order to enhance public safety a large number of PSNs have been introduced throughout the years. Nonetheless, these different technologies fail to coordinate and cooperate causing big problems to public safety operators. The reasons that interoperability remains a challenge are many, and include both technical and non-technical issues (e.g., governance, policies, procedures, and training) [158]. There are many cases which the failure of communication and data sharing among public safety networks costs money and more importantly human lives. Moreover, the use of multiple, potentially incompatible, technologies leads to interoperability problems [159].

It is important to mention that the need of interoperability becomes more necessary as the scale of the incident becomes more complex including more and more agencies. In Figure 6.1 we examine a scale of an incident from a local state to national. In national level the need of coordination and cooperation of public safety agencies becomes vital. As an incident grows in scale and complexity, integrating new agencies and personnel into the response becomes more challenging, and lack of interoperability between communications systems can result in slow and uneven distribution of information to the people and agencies in need of it [160].

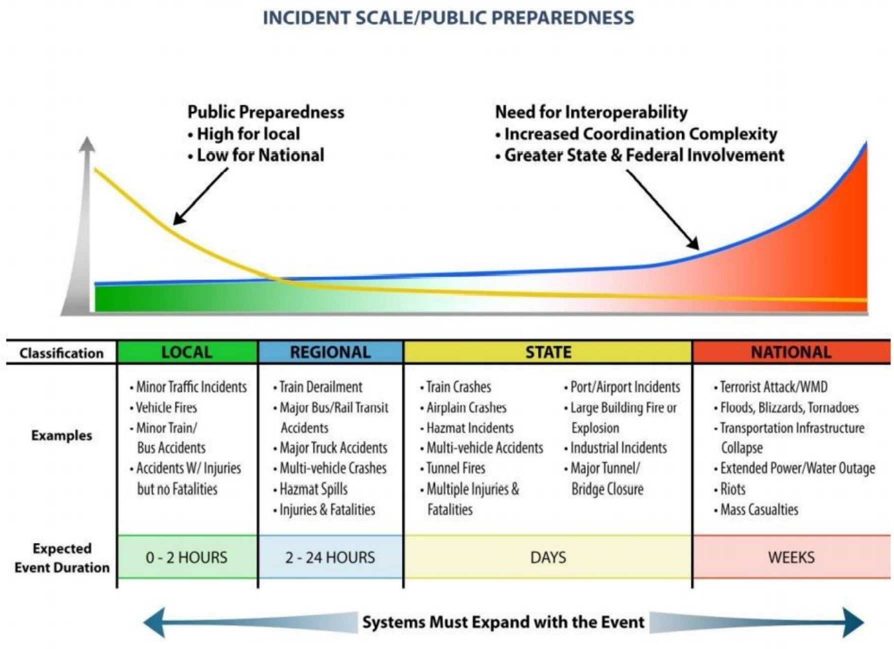

Figure 5.1: Incident scale and interoperability needs [160]

In order to resolve the issue of interoperability USA introduced FirstNet. FirstNet is capable of adopting broadband technologies to improve, enhance, and extend the effectiveness of emergency responders [161]. In other words FirstNet secures first responders communication and delivers interoperability between 2-way radios and smart phones. FirstNet is the only network that gives first responders *always-on*, 24-hours-a-day priority and preemption across voice and data [162].

5.2 Connectivity/reliability

Another important issue for public safety agencies is the lack of connectivity between their communication hardware/Software equipment. Different kinds of software or hardware devices public safety operators use, could easily lead to loss of communication. Loss of communication between public safety agencies during disasters is a serious matter as it may lead to human casualties. Recent disasters have emphasized the need to enhance interoperability, capacity and broadband connectivity of the wireless networks used by PS organizations [163]. Connectivity issue could be solved by the next generation of cellular networks which is represented by Long Term Evolution (LTE). LTE is able to provide broadband connectivity services dedicated specifically to the needs of public safety agencies. These services may include a priority call service or the transferring of emergency call data. Governments all over the world have gathered their recourses to enhance their reliability and connectivity among their public safety agencies. Any interruption in connectivity that delays critical information from getting where it is needed can put first responders, the public and property at risk [164].

5.3 Resource Scarceness - Network Congestion

PSNs have to deal with a large number of challenges during disasters. Two of them are the scarcity of existing communication technologies and the network congestion. Both of these problems make the work of public safety agencies extremely difficult. Nowadays, public safety networks share infrastructures and radio resources with commercial networks. Because of the mixture of two types of networks (commercial & public safety) a phenomenon which is called network congestion is occurred. This is particularly important in case of emergency situations. Consequently, public safety communications compete with general public communications with unpredictable effects on high priority emergency services [165]. It is important to research techniques to prevent as much as possible network congestion in order forPSNs to exchange critical information during emergency situations without any further delay.

Every public safety organization uses their own network infrastructure for its communication needs during emergency incidents. However, this fact may lead to resource scarceness. In future PSNs, sharing resources with commercial cellular networks can result in resource scarceness in disaster situations. Allocating more radio resources does not solve the problem of spectrum efficiency [166]. Different kinds of networks and radio resources with different kinds of communication techniques make the work of public safety agencies very hard to deliver. The large variety of resources does not guarantee the full availability of services PSNs deliver. A future and more convenient direction to resolve this issue can be the research of standards for unique communication ways among public safety agencies in order to avoid scarcity of resources.

5.4 Privacy & Security

Privacy and security of PSNs has been an extremely big issue since the beginning of their existence. Therefore, PSNs are extremely vulnerable from malicious attacks. Different communication technologies public safety agencies use and interoperability between them leads to security threats. Network sharing with commercial cellular networks will further tighten security requirements in PSNs. In shared networks, PS services must have their own mechanism for user authentication and authorization, which should be managed by PS service providers [166]. It is also important to mention that there are many factors that make the design of PSNs very challenging. The need for privacy and security in PSNs is extremely vital. Moreover, PSNs carry information for all the public safety agencies personnel (Firefighters, police officers, EMS). In order to achieve security and privacy for their operational and personal data public from outside threats public safety agencies design their PSNs with a number of requirements. Some of them are [167]:

- Protection against corrupted information: Accurate information sent to first responders. Critical information which is sent to first responders must be exactly the same without any changes.
- Protection against Denial of Service (DoS): Attackers execute DoS attacks to a PSN. In order for a PSN to prevent this, it must be architected to provide redundancy, detect and isolate these threats.
- Protection against data exfiltration: Protection of IDs and passwords as well as their personal profiles inside a PSN.
- Authentication and Acknowledgement: In order to ensure that only legitimate communication occurs across the public safety network, senders must be authenticated and acknowledgement must be sent when data is received. Authentication of the sender ensures that the information which is sent is genuine.

Furthermore, the involvement of drones raises new security issues in public safety networks [168]. Protection of data is extremely difficult and the information UAVs carry is vulnerable to outside threats. These security threats in drone-assisted PSNs include passive attacks and active attacks. Passive attacks include interception and modification of critical data. On the other hand, active attacks include DoS and message forgery (Figure 6.2).

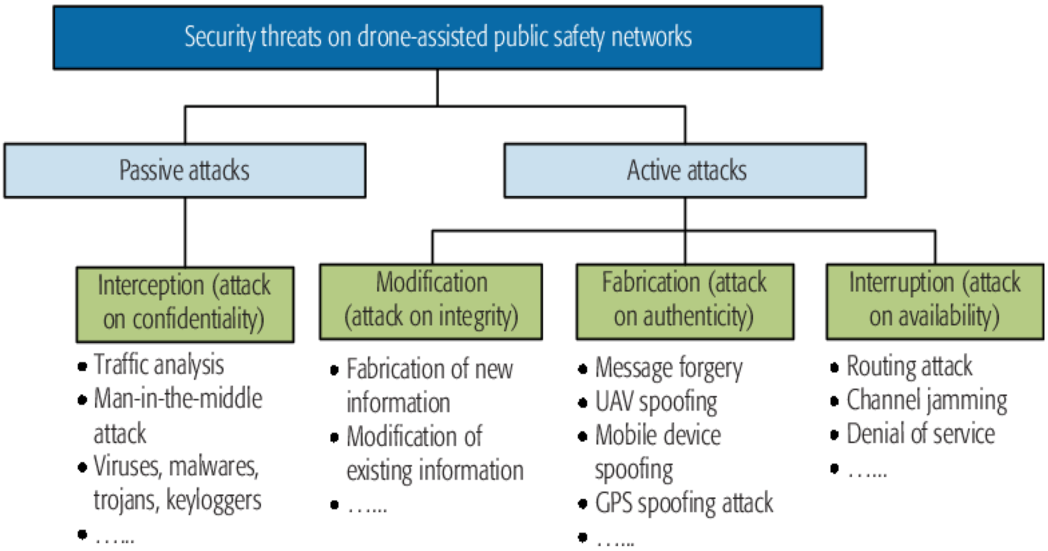

Figure 5.2: Security threats on the drone-assisted PSNs [168]

5.5 *Big Data - Data Analytics/Run time analytics*

Big Data is expected to play a key role in the operation of public safety organizations. In order for PSNs to deliver their services more efficiently they must use all of the groundbreaking technologies. One of them is the Big Data analytics. PSNs use a large variety of applications during emergency incidents to gather critical data, from body-worn cameras first responders use to traffic cameras situated in roads. Gathering data from social media is another aspect that we must take into consideration. The overall potential of efficiently analyzing even a small portion of the available data is immense [169]. History of Big Data analysis in terms of PSNs has proven to be extremely valuable. As an example, analysis of crime historical data is proved valuable in predicting how to effectively deploy officers [170]. Big Data analysis has been helpful for PSNs for crime prediction and prevention by constructing crime patterns.

However, analysis of Big Data to extract valuable information can be a challenging task. Analyzing big datasets could take a long time and when public safety officers have to face disasters time is not by their side. The most considerable challenge for implementing Big Data to public safety needs is to optimize the runtime analysis of large-scale datasets, for faster and better decision making during calamities. However, many interested public safety organizations lack the computing power and software tools required to integrate, analyze, and visualize Big Data [171]. Aspects such as data storage, computing power and specialized personnel (data scientists) are essential in order to optimize run time analysis of Big Data for public safety needs.

5.6 *Environmental conditions*

One of the key factors which affect the proper functionality of PSNs is about environmental conditions. PSNs and the public safety organizations they use them need to adapt and adjust to the changes of environmental conditions that may occur during their operations. Public safety management can be seriously affected by a number of extreme weather conditions. In addition, severe storms, tropical cyclones, winter storms and high winds are the weather parameters with the greatest effects on emergency management [172]. Network infrastructure must be protected in order for public safety agencies to communicate efficiently during crisis situations.

Recently, emergency managers depend on weather forecasts and observational weather data in order to protect critical communication infrastructure and improve their emergency response. Moreover, more and public safety organizations tend to observe meteorological data during the formation of an emergency response plan.

5.7 Cost effectiveness

Nowadays, public safety organizations invest a lot of money in order to upgrade their communication technologies. By upgrading their communication capabilities they are able to provide their services to the public more efficiently. Communications investments are among the most significant, substantial, and long-lasting capital expenditures that public safety agencies make [173]. However many of the new technologies public safety organizations invest are not cost effective and have no significant value to their users. This remains until today an open issue for the operation of public safety agencies. New technologies don't always guarantee the desired results as they require a lot of money for maintenance and don't make the work of first responders easier.

Cost effectiveness is one of the many reason public safety organizations fail to upgrade and evolve in terms of communications. In addition, PS communications still primarily use land mobile radio (LMR) system standards, such as Project 25 (P25) and terrestrial trunked radio (TETRA) [174] . These communication technologies are still used for a number of reasons. They are reliable, cost effective and tested many times in real time scenarios for mission critical voice applications. Cost effectiveness is serious factors that must be taken into seriously into account by the governments and public safety agencies as it ensures the survivability of a PSN especially during a disaster scenario.

5.8 Fault tolerance

It is vital that crisis situations PSNs will continue to work without interruption even though one or more of their components fail. A fail in communication among public safety agencies may cost time, money and more importantly human lives. One of the main challenges for public safety organization is to build fault-tolerant PSNs which will withstand any component system failure and ensure no loss of service. Fault tolerance can play a role in a disaster recovery strategy. For example, fault-tolerant systems with backup components in the cloud can restore mission-critical systems quickly, even if a natural or human-induced disaster destroys on-premise IT infrastructure [175].

PSNs which are fault tolerant have the privilege to maintain essential functions for public safety agencies during a disaster. However designing fault tolerant PSNs can be a difficult task. Certain factors must be taken into account. Two of them are cost and testing. Cost is one of the biggest disadvantages for adopting a fault-tolerant PSN. Fault-tolerant systems require organizations to have multiple versions of system components to ensure redundancy, extra equipment like backup generators, and additional hardware. These components need regular maintenance and testing. They also take up valuable space in data centers [176]. The second one is testing. A fault-tolerant PSN requires constant testing of its components and their correct functionality. Components must be continuously tested for performing to the expected level.

5.9 Dedicated Spectrum

First responders and public safety agencies need their own network infrastructure in order to communicate with each other especially in large-scale disasters. In many cases public demand for cellular networks is jamming the functionality of PSNs. During disasters heavy public use leads to wireless communication networks becoming unable to use. Public safety users as commercial users have limited communication capability due to congestion and capacity issuers. Therefore, a need for a dedicated network with dedicated frequencies for public safety needs is one of the main challenges governments and public safety organizations have to face permanently. The primary reason governments look to utilize existing commercial networks as a basis for their PSNs is the promise of cost-efficiency [178]. The use of commercial networks is extremely unreliable and risky and most likely could cost lives in disaster scenarios due to difficulty of communication. Commercial networks are designed for different needs and different situations compared to dedicated networks which are designed exactly for the needs of public safety (Figure 5.3).

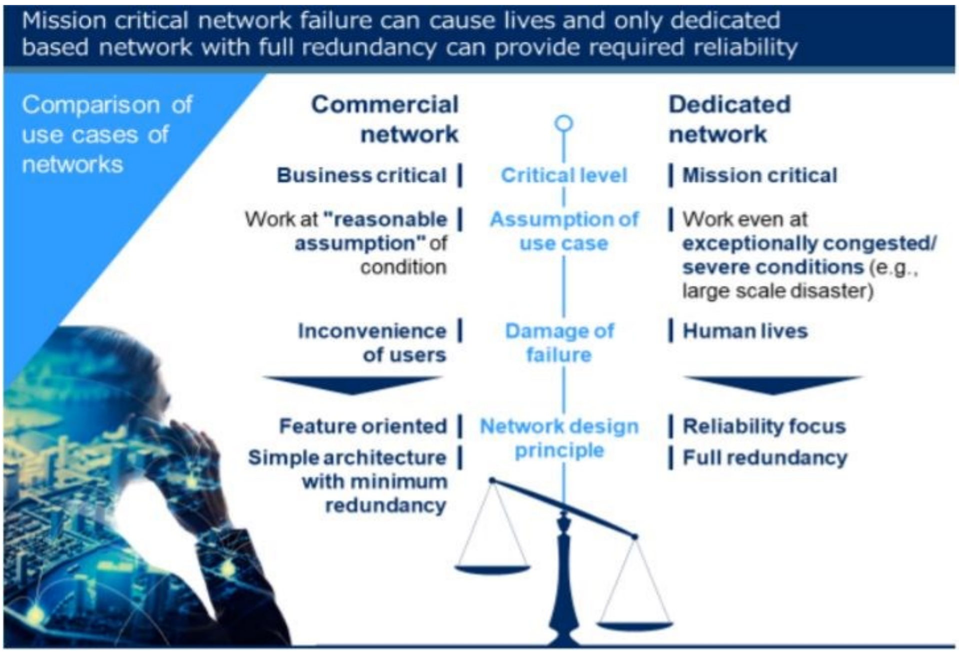

Figure 5.3: Fundamental differences between commercial and dedicated networks [178]

However, a dedicated spectrum for communication needs in public safety also brings an amount of difficulties. In case dedicated spectrum is used that is otherwise not used for public services means that devices with receivers for dedicated spectrum are required. In other words no mass products can be used which is always a cost driver [184].

During crisis situations PSNs need to communicate in dedicated networks exclusively for the needs of public safety. In USA, the need for a first responder network with dedicated spectrum was recognized in the wake of September 11^{th} in 2001, after first responders found it difficult to communicate on the congested cell phone network [177]. An answer to this problem is FirstNet. With the FirstNet Network, public safety gets a dedicated "fast lane" that provides highly secure communications every day and for every emergency [179]. FirstNet delivers vital features to public safety users such as priority access more network capacity and a resilient connection.

5.10 Moving cells and network mobility

Public safety agencies face the ultimate challenge of designing field communications with high mobility during critical situations. Moreover, field communications must be deployed in a way that provides network access and coverage on scene to all first responders. The technology which is currently used by public safety agencies is the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) which operates as the radio technology used between mobile terminals and the base stations of 3GPPTM systems Radio. E-UTRAN is considered fixed and detection as well as discovery of a network while moving cells are being deployed, remains unspecified [180]. However, when high mobility is achieved, another problem appears which is about network availability. Moving cells have limited network coverage so inter-cell discovery features must be enabled for proximity awareness. Proximity awareness gives the advantages of self-healing and intelligence to a PSN.

5.11 Programmability and flexibility

Programmability and flexibility are two main key factors of setting up the base of next generation smart PSNs. Both of these factors give the critical advantage to a PSN in responding to a variety of disaster scenarios with specific requirements and needs. PSN with such characteristics become more adaptable regarding the critical situation and provide valuable critical services which are required. Moreover, a high degree of programmable network components will be able to offer scalable and resilient network deployment on the-fly without the need of previous network planning by using network function virtualization and software-defined networking [180]. In addition, a PSN which is designed with high standards of programmability and flexibility is always able to visualize network infrastructure and create network services for first responders with flexible and intelligent control.

5.12 Location tracking

Currently public safety coordinators face difficulties on locating first responders during crisis situations. Location tracking of a number of public safety users remains until today an open issue. Some agencies have improved the tracking process by attaching GPS tracking sensors to emergency vehicles, enabling dispatch to track a unit's location and send the closest unit available. Still, once responders leave their vehicles, they become disconnected and their location unknown [181]. The developed broadband PSN FirstNet in USA has the advantage to provide the first responders with location services. Through this network which can carry high speed data like images and videos, first responders can pinpoint their exact location during disasters. Another technology which can aid dealing with the issue of location tracking is GIS (Geographic Information System). By making use of GIS, the control center can track where public safety agents are located and group agents together based on their location (Geo Fencing) [182].

5.13 Optimization of performance metrics to support sufficient QoS

A PSN must always be able to provide its services even if a component faces interruption or backhaul connectivity. In addition, a PSN especially during large-scale disasters requires a mechanism to invoke the appropriate complementary resources (e.g. additional bandwidth, alternate communication links, and complementary bearers) for self-healing operation and re-establishment of disrupted end-to-end bearers [180]. It is for the operation of a PSN that the same mechanism is in place to take critical decisions during disasters taking into account not only the availability of the resources but also the metrics of the communication performance. These metrics may include latency and spectral efficiency. Public safety agencies with the use of these metrics are able to improve their operational capabilities and provide more efficient services (QoS) during critical situations. By measuring the communication performance of a PSN sets the base of future improvements.

5.14 Traffic steering and scheduling

Recently, one of the biggest challenges of PSNs is traffic steering. Traffic steering is a technique applied to network traffic when additional filtering, modification or optimization is needed [183]. A component of the PSN is selected to steer the data traffic. Through this technique public safety users are able to connect the best fitted network which matches their

QoS requirements. Aiming at overall network optimization, traffic steering techniques can be leveraged to balance the network load and satisfy carrier and user demands by properly enabling data offloading, interference management or energy saving policies [180].

5.15 Network Infrastructure Replacement Cycles

New generation of hardware forces the upgrading of PSNs and radio base stations every 5 years approximately. New generation of public safety hardware has the ability to handle higher data rates. For this reason they consume and require less power, they are more efficient and smaller in size. Therefore the upgrading of the current network infrastructure becomes inevitable. Network infrastructure must be upgraded to match the requirements of the new generation in order of keeping the efficiency of a PSN to an accepted operational level. In current Private Mobile Radios (PMRs) timeframes are conservative and network capacity is limited. New generation of hardware in PSNs and in extent in PMRs requires a lot of performance testing which is costly for governments and public safety organizations. PMRs tend to upgrade their network infrastructure cycles when the current equipment becomes obsolete and no longer match the requirements of public safety users. However this brings another problem to the table. In case a PMR upgrades its network infrastructure after 10 years when the current equipment no longer serves the public safety purposes, pain of upgrading at that point is even more severe. Technology has advanced so far and there will be many problems when going from very old hardware to the current generation [184].

5.16 Power saving

In the area of public safety power consumption of devices is one key designing factor and a challenge. In all communication technologies public safety agencies use, power consumption could make a huge difference. Release 17 by 3GPP (3rd Generation Partnership Project) brings a set of groundbreaking enhancements in the area of public safety applications and power consumption of devices first responders carry. 3GPP Release 17 will mark the next chapter in New Radio (NR) standardization. In Release 17 enhancements to the sidelink and proximity services are being introduced to support public safety applications, for example where emergency workers can benefit from direct device-to-device communication [185]. Handheld devices first responders carry will have sidelink power - saving features. Top priority of Release 17 is power - saving enhancements for device that are inactive or idle nodes in order to improve battery life. 3GPP release 17 is expected to be completed and given for use by the end of 2021.

5.17 Scalability

Network scalability refers to how well a network can handle sudden changes in workload brought about by sudden spikes or drops in the volume of data it processes [186]. We refer as spikes to the sudden loss of internet connection. Developing a PSN is full of designing challenges. Design must include a number of characteristics. A top feature of modern PSNs is scalability. PSNs should be designed and developed to be scalable in order to address the specific communication needs of public safety agencies. Scalability gives the advantage of robustness and resilience to a PSN. Moreover, PSN can adapt to different critical situations quick and efficiently providing adequate services.

5.18 D2D communications

Establishment of D2D communications can bring huge difference in the way a PSN operates. In critical situations wireless coverage and communication between first responders and mobile users must be maintained and protected at all costs.D2D communication is a technique that enables the direct communication of User Equipment (UE) when the parties are within range for direct communication[187].Many benefits can be obtained using D2D communications such as providing wireless coverage beyond cellular networks, reducing burdens on the core network, providing high-speed communications, and supporting device discovery in rescue missions [188]. Both D2D communications on the user side and DWN deployment on the network side can be integrated as orthogonal and complimentary solutions for a PSN [187]. D2D sets the base of critical communication between first responders, independent of the current network infrastructure and outside of coverage areas or areas with limited network capacity. To enable D2D, 3GPP has standardized the concept of Proximity Service (ProSe)that can establish the communication path directly between two or more public safetyProSe-enabled UEs.

5.19 SDR and Cognitive Radio (technical & operational challenges)

Recently, several large-scale disasters motivated public safety agencies on how to evolve and use the SDR and Cognitive Radio technology in order to face critical communication challenges. One of these challenges is interoperability. First responders from different public safety agencies fail to communicate efficiently. SDR and Cognitive radio achieves interoperability in a simple way. Radio operating parameters such as frequency band, modulation type, and power are controlled by software [158]. Software which is reconfigurable allows radios used by first responders to be more flexible during critical situations and support multiple frequency bands.

6 Conclusions and Future Work

6.1 Conclusions

The main objective of the current thesis is the study and research of communication technologies for prediction and monitoring of disasters (natural & man-made) and emergency situations. After discussing in detail all kinds of disasters (natural &man-made), we also refer to the importance of critical communication services as well as critical communication users. In addition, we refer to applications used by public safety organizations their characteristics and their functional requirements. Furthermore, we discuss about the current hardware used by end users in emergency situations. Hardware such as UAVs and wearables give critical advantages to first responders during crisis situations. There has been an extensive report on narrowband and broadband networks used by public safety agencies as well as a number of communication techniques. The primary goal of every technique is the increase in operational efficiency of public safety users in the field. In addition, techniques such as AI and Data analytics are becoming powerful tools in the hands of public safety officers.

Moreover, the current thesis emphasized to the importance of disaster management and the upcoming 5^{th} generation of cellular technology. 5G and in particular 5G NR is expected to bring revolutionary changes in the way public safety users operate in critical situations. In addition, various use cases and scenarios of public safety and their communication technologies are discussed in detail too. Moreover, last chapter includes an analysis of challenges and open issues concerning the operational and functional requirements of PSNs. Many countries simply lack the infrastructure and funds to support emerging technologies for public safety. New technologies demand improvements to the current grid, improvements which could prove to be extremely expensive specifically for countries not being a part of EU. This results to having a great number of countries using obsolete technology and not be able to upgrade to the latest technology. In addition, the need for interoperability in PSNs is greater than ever. The large amount of communication technologies and techniques used by different public safety agencies has caused great difficulties in terms of coordination and cooperation during disasters. A viable solution to this matter is given by USA with the establishment of FirstNet. A communication platform capable of coordinating different public safety agencies.

Lack of hardware and software connectivity between public safety agencies is a serious matter as it leads to loss of communication in the field for first responders. Furthermore, the adaptability of new technologies is still a big issue for public safety. More and more public safety users simply lack the knowledge to use new technologies, either to lack of training or lack of scientific knowledge. As mentioned earlier, 5G will change dramatically the way public safety organizations operate. In addition, 5G brings faster adoption of IoT technology. This combined with the continuous improvement of AI will give a massive advantage to first responders. First responders will be able to receive and analyze critical information about an incident from all kinds of devices giving them better situational awareness.

6.2 Future work

The current thesis discussed in detail only a certain number of use-cases of public safety where communication technologies are used by public safety agencies. Moreover, we mainly emphasized in man-made disasters, their complexity as well as their impact on humanity. The other big category of disasters (natural disasters) also includes a large variety of examples worthy of researching and discussing in detail. In addition, we have also referred to several computing and communication technologies used by public safety in emergencies. Furthermore, there is still a big number of technologies implemented in various public safety use cases yet to be discussed. In addition, there are several emerging technologies connected to public safety worth mentioning and researching. The current thesis also referred to several operational challenges and open issues of PSNs. Once again, these challenges were only a small portion, as new issues and problems appear every day due to the rapid evolution of communication technologies. New open issues and challenges could be addressed to a future thesis with the same subject of scientific research.

.

References

[1] https://www.ifrc.org/" "What is disaster?",[Online]Available: https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/,[Accesed:20-August-2021]

[2] https://www.usgs.gov/ "How can climate change affect climate disasters",[Online]Available: https://www.usgs.gov/faqs/how-can-climate-change-affect-natural-disasters-1?qt-news_science_products=0#qt-news_science_products/,[Accesed:20-August-2021]

[3] https://eena.org/blog/critical-communications-today-and-tomorrow/.[Online]. Available: [Accessed: 20-July-2021]

[4] https://www.ifrc.org/en/what-we-do/disaster-management/about-disaster-management/,[Online]. Available: [Accessed: 20-July-2021]

[5] Daniel Câmara, Navid Nikaein, Wireless Public Safety Networks 2,Elsevier,2016,ISBN 9781785480522,https://doi.org/10.1016/B978-1-78548-052-2.50014-1.

[6] Arun Handa,System Engineering For IMS Networks,Newnes,2009,Pages xv-xix,ISBN 9780750683883

[7] White Paper ,Cradlepoint, Trends in Connected Technologies for First Responders,2019

[8] Fundamentals of Public Safety Networks and Critical Communications Systems: Technologies, Deployment, and Management, First Edition. Mehmet Ulema, by the Institute of Electrical and Electronics Engineers, Inc. Published by John Wiley & Sons,2019

[9] https://www.fortlauderdale.gov/ "About Ocean Rescue", [Online]. Available:https://www.fortlauderdale.gov/departments/fire-rescue/ocean-rescue/about-ocean-rescue.[Accessed: 14-July-2021]

[10] https://www.securelandcommunications.com/"10 brilliant public safety apps for professional", [Online]Available: https://www.securelandcommunications.com/blog/10-brilliant-public-safety-apps-for-the-professional#74c2c86b,[Accesed:21-August-2021]

[11] https://www.intelligence-airbusds.com/"Airbus - SAFEcommand app" ,[Online]:Availabe: https://www.intelligence-airbusds.com/markets/security/safecommand/ ,[Accesed:21-August-2021]

[12] https://tcconnect.se/"Tactilon Agnet" [Online]: Availabe: https://tcconnect.se/wp-content/uploads/2019/06/AIRBUS_Tactilon_Agnet_Brochure_EN_April_2018.pdf ,[Accesed:21-August-2021]

[13] https://www.securelandcommunications.com/"Which 3 requirements must mission critical communications meet?",[Online]:Availabe:https://www.securelandcommunications.com/blog/which-3-requirements-must-mission-critical-communications-meet#74c2c86b, [Accesed:21-August-2021]

[14] https://www.theagilityeffect.com/"Critical communications: New standards for private mobile radios", [Online]: Available: https://www.theagilityeffect.com/en/article/critical-communications-new-standards-for-private-mobile-networks/[Accesed:21-August-2021]

[15] M. Portmann and A. A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications," in *IEEE Internet Computing*, vol. 12, no. 1, pp. 18-25, Jan.-Feb. 2008, doi: 10.1109/MIC.2008.25.

[16] K. N. Sunil Kumar and Shivas hankar, "A review on security and privacy issues in wireless sensor networks," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017, pp. 1979-1984, doi: 10.1109/RTEICT.2017.8256945.

[17] hacko S, Job D ,Security mechanism and vulnerabilities in LPWAN. In: IOP conference series: materials science and engineering 396012027, November 2018

[18] M. Abbasi, S. Khorasanian and M. H. Yaghmaee, "Low-Power Wide Area Network (LPWAN) for Smart grid: An in-depth study on LoRaWAN," *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, 2019, pp. 022-029, doi: 10.1109/KBEI.2019.8735089.

[19] Martin, Jim and J. Westall. , "Evaluating WiMAX for Public Safety.", 2010

[20] https://www.fcc.gov/"WiMAX application for public safety", [Online] Available: https://www.fcc.gov/general/wimax-applications-public-safety, [Accessed:21-Aug-2021]

[21] https://www.corneralliance.com/Personal area networks , First responders and the power of data", [Online] Available: https://www.corneralliance.com/blog/personal-area-networks-first-responders-and-the-power-of-data, [Accessed:22-Aug-2021]

[22] https://www.lairdconnect.com/"ZigBee vs 6loWPAN for sensor networks", [Online] Available: https://www.lairdconnect.com/resources/white-papers/zigbee-vs-6lowpan-for-sensor-networks, [Accessed:22-Aug-2021]

[23] Leonard E. Miller, Wireless Technologies and the SAFECOM SoR for Public Safety Communications, Wireless Communication Technologies Group Advanced Network Technologies Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, Maryland, 2005

[24] H. Wang, L. Dong, W. Wei, W. Zhao, K. Xu and G. Wang, "The WSN Monitoring System for Large Outdoor Advertising Boards Based on ZigBee and MEMS Sensor," in *IEEE Sensors Journal*, vol. 18, no. 3, pp. 1314-1323, 1 Feb.1, 2018, doi: 10.1109/JSEN.2017.2770324.

[25] https://searchmobilecomputing.techtarget.com/ "Wireless ad hoc network (WANET)",[Online]Available:https://searchmobilecomputing.techtarget.com/definition/ad-hoc-network, [Accessed:23-Aug-2021]

[26] Devi, Munisha & Gill, Nasib. (2020). Novel Algorithm for Enhancing MANET Protocol in Smart Environment. 8. 1830-1835. 10.35940/ijitee.J9214.0881019.

[27] https://artes.esa.int/"Mobile ad hoc networks bolster public safety operations" Online] Available: https://artes.esa.int/news/mobile-ad-hoc-networks-bolster-public-safety-operations, [Accessed:23-Aug-2021]

[28] C. M. Raut and S. R. Devane, "Intelligent transportation system for smartcity using VANET," *2017 International Conference on Communication and Signal Processing (ICCSP)*, 2017, pp. 1602-1605, doi: 10.1109/ICCSP.2017.8286659.

[29] https://insights.samsung.com/"Wearable improves police awareness and safety", [Online] Available: https://insights.samsung.com/2019/11/12/wearable-tech-improves-police-awareness-and-safety-2/, [Accessed: 20-Aug-2021]

[30] https://www.criticalcomms.com/" Wearables for public safety: smart watches and smart glasses", [Online] Available: https://www.criticalcomms.com/features/public-safety-wearables-smart-watches-smart-glasses, [Accessed: 20-Aug-2021]

[31] https://www.travelers.com/"6 Ways Public Entities Use Smart Tech for Public Safety", [Online] Available: https://www.travelers.com/resources/business-industries/technology/ways-public-entities-use-smart-tech-for-public-safety, [Accessed: 21-Aug-2021]

[32] https://www.commercialuavnews.com/"Where are We Today with Drones in Public Safety?",[Online] Available: https://www.commercialuavnews.com/public-safety/drones-in-public-safety, [Accessed: 22-Aug-2021]

[33] S. Shakoor, Z. Kaleem, M. I. Baig, O. Chughtai, T. Q. Duong and L. D. Nguyen, "Role of UAVs in Public Safety Communications: Energy Efficiency Perspective," in *IEEE Access*, vol. 7, pp. 140665-140679, 2019, doi: 10.1109/ACCESS.2019.2942206.

[34] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, et al., "Survey on UAV cellular communications: Practical aspects standardization advancements regulation and security challenges", *IEEE Commun. Surveys Tuts.*

[35] L. D. Nguyen, K. K. Nguyen, A. Kortun and T. Q. Duong, "Real-time deployment and resource allocation for distributed UAV systems in disaster relief", *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, pp. 1-5, Jul. 2019.

[36] Franklin, J. , Howell, G. , Ledgerwood, S. and Griffith, J. (2020), Security Analysis of First Responder Mobile and Wearable Devices, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8196 (Accessed August 22, 2021)

[37] https://www.criticalcomms.com/,"Wearable sensors for monitoring heat stress", [Online] Available: https://www.criticalcomms.com/features/wearables-biometrics-firefighters-heat-stress, [Accessed: 23-Aug-2021]

[38] Hager, Gregory & Kumar, Vijay & Murphy, Robin & Rus, Daniela & Taylor, Russell. (2020). The Role of Robotics in Infectious Disease Crises.

[39] https://robotnik.eu/,"All that robotics brings to security and rescue", [Online] Available: https://robotnik.eu/all-that-robotics-brings-to-security-rescue/, [Accessed: 24-Aug-2021]

[40] Michelle Wetterwald, Damien Saucez, Xuan-Nam Nguyen, Thierry Turletti. SDN for Public Safety Networks. [Research Report] Inria Sophia Antipolis. 2016. ffhal-01400746f

[41] https://www.vmware.com/"Network Functions Virtualization (NFV)", [Online] Available: https://www.vmware.com/topics/glossary/content/network-functions-virtualization-nfv, [Accessed: 24-Aug-2021]

[42] https://www.ericsson.com/,"Network slicing accelerates 5G for business", [Online] Available: https://www.ericsson.com/en/network-slicing?gclsrc=aw.ds&gclid=Cj0KCQjwg7KJBhDyARIsAHrAXaHLgE6WhHZgl3gPat1rhKSEZGLDx-z4XXJVMvGaJ6nXxqz5phkE248aAhYPEALw_wcB, [Accessed: 24-Aug-2021]

[43] https://www.comtechlocation.com/"5G from public safety requirements to Network slice", [Online] Available: https://www.comtechlocation.com/blog/5g-from-public-safety-requirements-to-network-slice, [Accessed: 24-Aug-2021]

[44] https://www.euromoney.com/"What is blockchain?", [Online] Available: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain, [Accessed: 24-Aug-2021]

[45] https://gcn.com/"How blockchain can improve public safety", [Online] Available: https://gcn.com/articles/2019/04/17/blockchain-public-safety.aspx,[Accessed: 24-Aug-2021]

[46] Henman, Paul. (2020), Improving public services using artificial intelligence: possibilities, pitfalls, governance. Asia Pacific Journal of Public Administration. 42. 1-13. 10.1080/23276665.2020.1816188.

[47] https://www.csc.gov.sg/" Artificial Intelligence: Impact on Public Safety and Security", [Online] Available: https://www.csc.gov.sg/articles/artificial-intelligence-impact-on-public-safety-and-security, [Accessed: 24-Aug-2021]

[48] https://eena.org/"Artificial Intelligence and Machine Learning in public safety", [Online] Available: https://eena.org/knowledge-hub/documents/artificial-intelligence-machine-learning-in-public-safety/, [Accessed: 24-Aug-2021]

[49] X. Song *et al*., "Big Data and Emergency Management: Concepts, Methodologies, and Applications," in *IEEE Transactions on Big Data*, doi: 10.1109/TBDATA.2020.2972871.

[50] S. A. Shah, D. Z. Seker, S. Hameed and D. Draheim, "The Rising Role of Big Data Analytics and IoT in Disaster Management: Recent Advances, Taxonomy and Prospects," in *IEEE Access*, vol. 7, pp. 54595-54614, 2019, doi: 10.1109/ACCESS.2019.2913340.

[51] P. Mikalef, I. O. Pappas, J. Krogstie and M. Giannakos, "Big data analytics capabilities: A systematic literature review and research agenda", *Inf. Syst. e-Bus. Manage.*, vol. 16, no. 3, pp. 547-578, 2018.

[52] https://www.etsi.org/,"EXTENDED REALITY: AR,VR.XR.MR AT A GLANCE", [Online] Available: https://www.etsi.org/images/files/ETSITechnologyLeaflets/eXtended-Reality.pdf, [Accessed: 25-Aug-2021]

[53] https://phys.org/. "NIST virtual reality aims to win for public safety", [Online] Available: https://phys.org/news/2018-05-nist-virtual-reality-aims-safety.html, [Accessed: 25-Aug-2021]

[54] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014

[55] Q. Chen *et al*., "A Survey on an Emerging Area: Deep Learning for Smart City Data," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 3, no. 5, pp. 392-410, Oct. 2019, doi: 10.1109/TETCI.2019.2907718.

[56] https://statetechmagazine.com/"How 5G and Multi-Access Edge Computing Can Optimize Public Safety," [Online]

Available:https://statetechmagazine.com/article/2019/03/how-5g-and-multi-access-edge-computing-can-optimize-public-safety-perfcon, [Accessed: 25-Aug-2021]

[57] A. Rauniyar, P. Engelstad, B. Feng and D. V. Thanh, "Crowdsourcing-Based Disaster Management Using Fog Computing in Internet of Things Paradigm," *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, 2016, pp. 490-494, doi: 10.1109/CIC.2016.074.

[58] https://www.sam-solutions.com/"Fog computing vs Cloud computing for IoT projects", [Online] Available: https://www.sam-solutions.com/blog/fog-computing-vs-cloud-computing-for-iot-projects/, [Accessed: 25-Aug-2021]

[59] P. Rawat, M. Haddad and E. Altman, "Towards efficient disaster management: 5G and Device to Device communication," *2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2015, pp. 79-87, doi: 10.1109/ICT-DM.2015.7402056.

[60] A. Kumbhar, F. Koohifar, İ. Güvenç and B. Mueller, "A Survey on Legacy and Emerging Technologies for Public Safety Communications," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 97-124, Firstquarter 2017, doi: 10.1109/COMST.2016.2612223.

[61] A. Gorcin and H. Arslan, "Public safety and emergency case communications: Opportunities from the aspect of cognitive radio," in New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on. IEEE, 2008, pp. 1–10.

[62] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," Communications Magazine, IEEE, vol. 49, no. 3, pp. 74–81, 2011.

[63] T. Doumi *et al.*, "LTE for public safety networks," in *IEEE Communications Magazine*, vol. 51, no. 2, pp. 106-112, February 2013, doi: 10.1109/MCOM.2013.6461193.

[64] https://www.brainbridge.be/" From 1G to 5G: A Brief History of the Evolution of Mobile Standards", [Online] Available: https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, [Accessed: 3-Sep-2021]

[65] https://support.chinavasion.com/"1G, 2G, 3G, 4G - The Evolution of Wireless Generations", [Online] Available: https://support.chinavasion.com/index.php?/Knowledgebase/Article/View/284/42/1g-2g-3g-4g---the-evolution-of-wireless-generations, [Accessed: 2-Sep-2021]

[66] Camara, Daniel &Nikaein, N.. (2015). Wireless Public Safety Networks 1: Overview and Challenges.

[67] https://tcca.info/"4G and 5G for Public Safety Technology Options", [Online] Available: https://tcca.info/documents/2017-march_tcca_4g_and_5g_for_-public_safety.pdf/, [Accessed: 3-Sep-2021]

[68] https://www.5gtechnologyworld.com/, “The impacts of 5G on the future: A new era of connectivity”, [Online] Available: https://www.5gtechnologyworld.com/the-impacts-of-5g-on-the-future-a-new-era-of-connectivity/, [Accessed: 3-Sep-2021]

[69] https://www.a10networks.com/”What is 5G?”, [Online] Available: https://www.a10networks.com/blog/what-is-5g/, [Accessed: 4-Sep-2021]

[70] P. Rawat, M. Haddad and E. Altman, "Towards efficient disaster management: 5G and Device to Device communication," *2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2015, pp. 79-87, doi: 10.1109/ICT-DM.2015.7402056.

[71] C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola and C. Fischione, "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3607-3644, Fourthquarter 2018, doi: 10.1109/COMST.2018.2855063.

[72] https://www.rfpage.com/”What is 5G NR (new radio) and how it works”, [Online] Available: https://www.rfpage.com/what-is-5g-nr-new-radio-and-how-it-works/, [Accessed: 4-Sep-2021]

[73] X. Lin *et al*., "5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology," in *IEEE Communications Standards Magazine*, vol. 3, no. 3, pp. 30-37, September 2019, doi: 10.1109/MCOMSTD.001.1800036.

[74] https://www.qualcomm.com/”Making 5G NR a reality”, [Online] Available: https://www.qualcomm.com/media/documents/files/making-5g-nr-a-reality.pdf, [Accessed: 4-Sep-2021]

[75] Muhammad Arslan, Ana Roxin, Christophe Cruz, Dominique Ginhac. A Review on Applications of Big Data for Disaster Management. The 13th International Conference on SIGNAL IMAGE TECHNOLOGY & INTERNET BASED SYSTEMS, Dec 2017, Jaipur, India. ffhal-01678238f

[76] *https://www.fema.gov,* “*Emergency Managementin the United States*”. [Online]. Availabe:https://training.fema.gov/emiweb/downloads/is111_unit%204.pdf[Accesed: 1-June-2021]

[77] Crystal Kwan and Christine A. Walsh, Seniors’ disaster resilience: A scoping review of the literature, International Journal of Disaster Risk Reduction, http://dx.doi.org/10.1016/j.ijdrr.2017.09.010

[78] www.ems.gov, “what is EMS?” [Online]. Availabe: https://www.ems.gov/whatisems.html. [Accesed: 25-Mar-2021]

[79] Albert Y. Chen, Ting-Yi Yu, Network based temporary facility location for the Emergency Medical Services considering the disaster induced demand and the transportation infrastructure in disaster response, Volume 91,2016, Pages 408-423

[80] M. A. Usman, N. Y. Philip and C. Politis, "5G Enabled Mobile Healthcare for Ambulances," *2019 IEEE Globecom Workshops (GC Wkshps)*,Waikoloa,HI,USA.pp.1-6

[81] A Vision on Intelligent Medical Service for Emergency on 5G and 6G Communication Era,2020

[82] D. G.C., A. Ladas, Y. A. Sambo, H. Pervaiz, C. Politis and M. A. Imran, "An Overview of Post-Disaster Emergency Communication Systems in the Future Networks," in *IEEE Wireless Communications*, vol. 26, no. 6, pp. 132-139, December 2019, doi: 10.1109/MWC.2019.1800467.

[83] Ahad A, Tahir M, Aman Sheikh M, Ahmed KI, Mughees A, Numani A. Technologies Trend towards 5G Network for Smart Health-Care Using IoT: A Review. Sensors (Basel). 2020 Jul 21

[84] C. Yang, G. Su and J. Chen, "Using big data to enhance crisis response and disaster resilience for a smart city," *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, Beijing, China, 2017

[85] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu and F. Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1578-1586, May 2014

[86] Besaleva , CrowdHelp: M-Health application for emergency response improvement through crowdsourced and sensor-detected information,2014

[87] Vikash Yadav, Humanitarian Impact of Drones in Healthcare and Disaster Management, January 2019

[88] Nonthapatpulshiri, Save lives: A review of ambulance Technologies in pre-hospital emergency medical services ,2019

[89] J. Rexiline Ragini, P.M. Rubesh Anand, VidhyacharanBhaskar,Big data analytics for disaster response and recovery through sentiment analysis,International Journal of Information Management, Volume 42, Pages 13-24, 2018

[90] J. Wang, Y. Wu, N. Yen, S. Guo and Z. Cheng, "Big Data Analytics for Emergency Communication Networks: A Survey," in *IEEE Communications Surveys &Tutorials*, vol. 18, no. 3, pp. 1758-1778, third quarter 2016, doi: 10.1109/COMST.2016.2540004.

[91] X. Song *et al*., "Big Data and Emergency Management: Concepts, Methodologies, and Applications," in *IEEE Transactions on Big Data*, doi: 10.1109/TBDATA.2020.2972871.

[92] R. W. Jones and G. Despotou, "Unmanned Aerial Systems and Healthcare: Possibilities and Challenges," *2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2019, pp. 189-194, doi: 10.1109/ICIEA.2019.8834142.

[93] R. Aringhieri, M.E. Bruni, S. Khodaparasti and J.T. van Essen, Emergency Medical Services and beyond: Addressing new challenges through a wide literature review, Computers and Operation Research, http://dx.doi.org/10.1016/j.cor.2016.09.016

[94] Abir M, Forman J, Taymour RK, Brent C, Nallamothu BK, Scott J, Wahl K. Optimizing Routine and Disaster Prehospital Care Through Improved Emergency Medical Services Oversight. Disaster Med Public Health Prep. 2020 Jun

[95] Christina L. Catlett, J. Lee Jenkins & Michael G. Millin (2011) Role of Emergency Medical Services in Disaster Response: Resource Document for the National Association of EMS Physicians Position Statement, Pre-hospital Emergency Care, 15:3, 420-425,

[96] Jaffe, E., Skornik, Y., Offenbacher, J., & Alpert, E. (2020). The Role of Emergency Medical Services in Earthquake Response: Integrating the ABC Approach of Israel's Magen David Adom. *Disaster Medicine and Public Health Preparedness,* 1-7. doi:10.1017/dmp.2020.124

[97] Abhijith H Va , S Deepak Rajb , Dr. H S Ramesh Babu, "Intelligent boundary determination of oil spill detection using IOT,2018

[98] Pu Li, Qinhong Cai, Weiyun Lin, Bing Chen ,Baiyu Zhang, Offshore oil spill response practices and emerging challenges,2016

[99] Marios Krestenitis, Georgios Orfanidis, Konstantinos Ioannidis, Konstantinos Avgerinakis, Stefanos Vrochidis and Ioannis Kompatsiaris, Oil Spill Identification from Satellite Images Using Deep Neural Networks,2019

[100] www.bsee.gov, "Oil spill Preparedness". [Online]. Availabe: https://www.bsee.gov/what-we-do/oil-spill-preparedness [Accesed: 2-Apr-2021]

[101] ZeyuJiaoa ,GuozhuJiaa , Yingjie Caib, A new approach to oil spill detection that combines deep learning with unmanned aerial vehicles,2018

[102] İrşad BAYIRHAN, Cem GAZİOĞLU, Use of Unmanned Aerial Vehicles (UAV) and Marine Environment Simulator in Oil Pollution Investigations,2020

[103] Thomas De Kerf ,JonaGladines , Seppe Sels and Steve Vanlanduit, Oil Spill Detection Using Machine Learning and Infrared Images,2020

[104] X. Li, P. Wan, H. Zhang, M. Li and Y. Jiang, "The Application Research of Internet of Things to Oil Pipeline Leak Detection," *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2018, pp. 211-214

[105] Capizzi, Giacomo & Sciuto, Grazia & Woźniak, Marcin &Damasevicius, Robertas. A Clustering Based System for Automated Oil Spill Detection by Satellite Remote Sensing,2016

[106] Chang, Stephanie & Stone, Jeremy & Demes, Kyle & Piscitelli-Doshkov, Marina. (2014). Consequences of oil spills: A review and framework for informing planning. ECOLOGY AND SOCIETY. 19. 26. 10.5751/ES-06406-190226.

[107] W. Alpers, B. Holt and K. Zeng, "Oil spill detection by imaging radars: Challenges and pitfalls," *2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, 2017, pp. 1522-1525, doi: 10.1109/IGARSS.2017.8127258.

[108] Tughral Yamin, Nuclear Disaster Management,2011

[109] https://www.world-nuclear.org/, "What are the effects of nuclear accidents?", [Online].Available : https://www.world-nuclear.org/nuclear-essentials/what-are-the-effects-of-nuclear-accidents.aspx [Accesed: 26-Apr-2021]

[110] T. Perko , Y. Tomkiv, I. Prezelj , M.C. Cantone , E. Gallego and D.H. Oughton, Communication with media in nuclear or radiological emergencies: general and practical recommendations for improvement,2016

[111] Akira Ohtsuru, Koichi Tanigawa, Atsushi Kumagai, Ohtsura Niwa, Noboru Takamura, Sanae Midorikawa, Kenneth Nollet, Shunichi Yamashita, Hitoshi Ohto, Rethy K Chhem, Mike Clarke ,Nuclear disasters and health: lessons learned, challenges, and proposals,2015

[112] Tanja Perko, Baldwin van Gorp, Catrinel Turcanu,1 Peter Thijssen, and Benny Carle, Communication in Nuclear Emergency Preparedness: A Closer Look at Information Reception,2013

[113] Min-Fan Ricky Tzu-Wei Chien, Artificial Intelligence and Internet of Things for Robotic Disaster Response,2020

[114] Ashwini S R, Dr. Shivashankar , Karthik R , Chethan , Harish B R , Karan D Bafna Wireless Sensors Network for Environmental Radiation Monitoring using IOT,2018

[115] Perko, Tanja &Tomkiv, Yevgeniya & Prezelj, Iztok & Cantone, M.C. & Gallego, Eduardo & Oughton, Deborah. (2016). Communication with media in nuclear or radiological emergencies: General and practical recommendations for improvement. Radioprotection. 51. S163-S169. 10.1051/radiopro/2016057.

[116] Marjan Malešič, Iztok Prezelj, Jelena Juvan, Marko Polič, Samo Uhan, Evacuation in the event of a nuclear disaster: Planned activity or improvisation?, International Journal of Disaster Risk Reduction,Volume 12,2015,Pages 102-111

[117] NasreddineBouhaï; Imad Saleh, "Tweets from Fukushima: Connected Sensors and Social Media for Dissemination after a Nuclear Accident," in *Internet of Things: Evolutions and Innovations*, Wiley, 2018, pp.169-187, doi: 10.1002/9781119427391.ch7.

[118] Nurul Hazwani Mohd Shamsuddin, Nor Azizah Ali , Razana Alwee An Overview on Crime Prediction Methods,2017

[119] Lawrence McClendon and Natarajan Meghanathan, Using Machine Learning Algorithms to Analyze crime data,2015

[120] P. Saskia Bayerl, Babak Akhgar, Ben Brewster, Konstantinos Domdouzis, Helen Gibson, Social media and its role for LEAs: Review and applications,2014

[121] Okereafor D. T., Diala U., Onuekwusi N., Uzoechi L.O., Chukwudebe G, Improving Security and Emergency Response Through the Use of Unmanned Vehicles,2013

[122] Ryan J. Wallace ,How Law Enforcement Unmanned Aircraft Systems (UAS) Could Improve Tactical Response tactical Response to Activ o Active Shooter Situations: The Case e Shooter Situations: The Case of the 2017 Las Vegas Shooting,2017

[123] Bogdan Ionescu , Razvan Roman, Marian Buric, Florin Rastoceanu, Marian Ghenescu , Artificial Intelligence Fights Crime and Terrorism at a New Level,2020

[124] Stelios Andreadis, Ilias Gialampoukidis, George Kalpakis, Theodora Tsikrika, Symeon Papadopoulos, Stefanos Vrochidis and Ioannis Kompatsiaris, A Monitoring Tool for Terrorism-related Key-players and Key-communities in Social Media Networks, 2017

[125] Thomas Heverin ,Lisl Zach Law enforcement agency adoption and use of Twitter as a crisis communication tool,2012

[126] Andrew J. Park, Houssem Zouaghi, Herbert H. Tsang, Crowd Control Strategy Framework Using Real-Time 3D Simulations,2018

[127] Neetu Singh, Chengappa Bellathanda Kaverappa, Jehan D. Joshi, Data Mining for Prevention of Crimes, 2018

[128] D.VIJAYA ROHINI, Dr.P.ISAKKI @ DEVI Crime Analysis and Mapping through Online Newspapers: A Survey,2016

[129] S. Raaijmakers, "Artificial Intelligence for Law Enforcement: Challenges and Opportunities," in *IEEE Security & Privacy*, vol. 17, no. 5, pp. 74-77, Sept.-Oct. 2019, doi: 10.1109/MSEC.2019.2925649.

[130] B. Panja, P. Meharia and K. Mannem, "Crime Analysis Mapping, Intrusion Detection - Using Data Mining," *2020 IEEE Technology & Engineering Management Conference (TEMSCON)*, 2020, pp. 1-5, doi: 10.1109/TEMSCON47658.2020.9140074.

[131] https://www.nhtsa.gov/,“Vehicle to Vehicle Communication”, [Online]Available: https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication [Accessed: 20-June-2021]

[132] M. Gupta, J. Benson, F. Patwa and R. Sandhu, "Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets," in *IEEE Transactions on Services Computing*, doi: 10.1109/TSC.2020.3025993.

[133] Fatma Outay, Faouzi Kamoun, Florent Kaisser, Doaa Alterri, Ansar Yasar,V2V and V2I Communications for Traffic Safety and CO2 Emission Reduction: A Performance Evaluation, Procedia Computer Science,Volume 151,2019,Pages 353-360

[134] Sven Eckelmann, Toralf Trautmann, Hagen Ußler, Benjamin Reichelt, Oliver Michler,V2V-Communication, LiDAR System and Positioning Sensors for Future Fusion Algorithms in Connected Vehicles, Transportation Research Procedia, Volume 27,2017,Pages 69-76,

[135] Ivan Lujic, Vincenzo De Maio, Klaus Pollhammer, Ivan Bodrozic, Josip Lasic, and Ivona Brandic. 2021. Increasing Traffic Safety with Real-Time Edge Analytics and 5G. In Proceedings of the 4th International Workshop on Edge Systems, Analytics and Networking (EdgeSys '21). Association for Computing Machinery, New York, NY, USA, 19–24. DOI:https://doi.org/10.1145/3434770.3459732

[136] M. C. Erturk, H. Jamal and D. W. Matolak, "Potential Future Aviation Communication Technologies," *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, 2019, pp. 1-10, doi: 10.1109/DASC43569.2019.9081679.

[137] https://cordis.europa.eu/,“Networking the sky with new aircraft communication technology”,[Online].Available: https://cordis.europa.eu/article/id/36558-networking-the-sky-with-new-aircraft-communication-technology [Accessed: 22-June-2021]

[138] Choi, Junsung & Marojevic, Vuk & Dietrich, Carl & Ahn, Seungyoung. (2021). DSRC-Enabled Train Safety Communication System at Unmanned Crossings.

[139] https://www.auto-talks.com/,”DSRC Technology”,[Online].Available: https://www.auto-talks.com/technology/dsrc-technology/[Accesed: 22-June-2021]

[140] J. Farooq and J. Soler, "Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1377-1402, thirdquarter 2017, doi: 10.1109/COMST.2017.2661384.

[141] https://www.ship-technology.com/, “Preventing ship collisions: Is technology the answer?”,[Online].Available:https://www.ship-technology.com/features/ship-collisions/,[Accessed: 25-May-2021]

[142] https://syncedreview.com/,”Fujitsu verifies AI technology to predict vessel collision risks in marine traffic control , improves maritime safety”[Online].Available:https://syncedreview.com/2020/04/23/fujitsu-verifies-ai-

technology-to-predict-vessel-collision-risks-in-marine-traffic-control-improves-maritime-safety/,[Accesed: 25-May-2021]

[143] https://study.com/, “Water & Recreational Safety: Definition and Precautionary Measures”,[Online].Available: https://study.com/academy/lesson/water-recreational-safety-definition-and-precautionary-measures.html,[Accesed: 25-May-2021]

[144] Wang, Tingxuan. "Study on intelligent stadiums system and development trend based on the internet of things." *RISTI* [RevistaIberica de Sistemas e Tecnologias de Informacao], no. E8, 2016, p. 80+.

[145] Syed Ahsan Raza Naqvi, Syed Ali Hassan, Haris Pervaiz, and Qiang Ni, Drone-Aided Communication as a Key Enabler for 5G and Resilient Public Safety Networks,2018

[146] K. Guevara, M. Rodriguez, N. Gallo, G. Velasco, K.Vasudeva, and I. Guvenc, UAV-Based GSM Network for Public Safety Communications,2015

[147] Rasoul Faraji, Mehrali Hemmatinezhad & Tracy Taylor (2018): Critical Factors Affecting Stadiums Security, Journal of Applied Security Research, DOI: 10.1080/19361610.2018.1498264

[148] Einavipour, Sina& Javidan, Reza. (2021). An intelligent IoT-based positioning system for theme parks. The Journal of Supercomputing. 10.1007/s11227-021-03669-9.

[149] https://blooloop.com/, “Theme park digital technology predictions for 2020”,[Online].Available:https://blooloop.com/theme-park/opinion/theme-park-digital-technology-predictions/[Accesed: 15-June-2021]

[150] https://www.ternplc.com/, “How IoT technology is being used in the theme park industry”,[Online].Available:https://www.ternplc.com/blog/how-iot-technology-is-being-used-in-the-theme-park-industry [Accesed: 15-June-2021]

[151] Athina Tsanousa, Vasileios-Rafail Xefteris, Dimos Ntioudis, Christos Chatzigeorgiou, Georgios Meditskos, Stefanos Vrochidis, IoannisKompatsiaris. (2020). Localization module for missing child scenario in IoT safety domains.

[152] https://blog.peakptt.com, “How IoT technology is being used in the theme park industry”,[Online].Available: https://blog.peakptt.com/push-to-talk-communication-for-amusement-park-management/ [Accesed: 15-June-2021]

[153] https://wdrfree.com/ “Natural disasters infographics set with sketch globe and catastrophe symbols vector illustration premium vector by macrovector”,[Online].Available:https://wdrfree.com/stock-vector/download/natural-disasters-infographics-79988758 [Accesed:20-Aug-2021]

[154] https://www.usnews.com/”10 of the deadliest natural disasters in 2018”,[Online].Available:https://www.usnews.com/news/best-

countries/slideshows/10-of-the-deadliest-natural-disasters-in-2018?slide=12,[Accesed:13-July-2021]

[155] https://blog.sscor.com/"4 types of natural disasters and their specific injuries",[Online].Available:https://blog.sscor.com/4-types-of-natural-disasters-and-their-specific-injuries,[Accesed:13-July-2021]

[156] https://www.ifrc.org/"Types of hazards: Definition of hazard",[Online].Available:https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/definition-of-hazard/,[Accesed:13-July-2021]

[157] https://qsstudy.com/ "Classification of Natural Disaster",[Online].Available:https://qsstudy.com/geology/classification-of-natural-disaster/,[Accesed:13-July-2021]

[158] Fred Frantz, L-3 Communications "SDR for Public Safety"

[159] Yipeng, et al., Organization of Public Safety Networks: Spillovers, Interoperability, and Participation. Production and Operations Management (2016), http://dx.doi.org/doi:10.1111/poms.12655

[160] Voss, B. and Anderson, E. (2019), Interoperability of real-time public safety data: Challenges and possible future states, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8255 (Accessed:July-11-2021)

[161] Linda K. Moore, The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress,2016

[162] https://about.att.com/" Let's talk about Interoperability",[Online].Available: https://about.att.com/innovationblog/2021/fn_interoperability.html [Accesed:20-June-2021]

[163] W. Yu, H. Xu, J. Nguyen, E. Blasch, A. Hematian and W. Gao, "Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions," in IEEE Access, vol. 6, pp. 70397-70425, 2018, doi: 10.1109/ACCESS.2018.2879760.

[164] https://www.smartcitiesworld.net/ "Public Safety Agencies increasingly reliant on connectedservices",[Online].Available:https://www.smartcitiesworld.net/news/news/public-safety-agencies-increasingly-reliant-on-connected-services-6041,[Accesed:1-August-2021]

[165] Marabissi, D. &Fantacci, R.. (2017). Heterogeneous Public Safety Network Architecture Based on RAN Slicing. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2768800.

[166] Imran, Muhammad & Sambo, Yusuf & Abbasi, Qammer. (2019). Enabling 5G Communication Systems to Support Vertical Industries. 10.1002/9781119515579.

[167] A. R. McGee, M. Coutière and M. E. Palamara, "Public safety network security considerations," in *Bell Labs Technical Journal*, vol. 17, no. 3, pp. 79-86, Dec. 2012, doi: 10.1002/bltj.21559.

[168] D. He, S. Chan and M. Guizani, "Drone-Assisted Public Safety Networks: The Security Aspect," in IEEE Communications Magazine, vol. 55, no. 8, pp. 218-223, Aug. 2017, doi: 10.1109/MCOM.2017.1600799CM.

[169] E. Biliri *et al*., "Big data analytics in public safety and personal security: Challenges and potential," *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 2017, pp. 1382-1386, doi: 10.1109/ICE.2017.8280043.

[170] IBM, "How analytics reduces crime and improves public safet," 2015. [Online]. Available: http://www.ibmbigdatahub.com/blog/howanalytics-reduces-crime-and-improves-public-safety,[Accesed:1-August-2021]

[171] Gamage, Pandula. (2016), New development: Leveraging 'big data' analytics in the public sector. Public Money & Management. 36. 385-390. 10.1080/09540962.2016.1194087.

[172] Pisano, P., L. Goodwin and A. Stern. "SURFACE TRANSPORTATION SAFETY AND OPERATIONS: THE IMPACTS OF WEATHER WITHIN THE CONTEXT OF CLIMATE CHANGE." (2003).

[173] SAFECOM NCSWIC, Emergency Communications Systems Value Analysis Guide,2020

[174] M. M. Sohul, M. Yao, X. Ma, E. Y. Imana, V. Marojevic and J. H. Reed, "Next generation public safety networks: A spectrum sharing approach," in *IEEE Communications Magazine*, vol. 54, no. 3, pp. 30-36, March 2016, doi: 10.1109/MCOM.2016.7432144.

[175] https://www.imperva.com/,"Fault Tolerance",[Online].Available:https://www.imperva.com/learn/availability/fault-tolerance/,[Accesed:2-August-2021]

[176] https://www.fortinet.com/" What is Fault Tolerance?",[Online].Available:https://www.fortinet.com/resources/cyberglossary/fault-tolerance/,[Accesed:2August-2021]

[177] https://www.digi.com/," What is FirstNet Band 14?",[Online].Available:https://www.digi.com/blog/post/what-is-firstnet-band-14/,[Accesed:3August2021]

[178] THE CASE FOR DEDICATED PUBLIC SAFETY NETWORKS WHY COMMERCIAL NETWORKS ARE NOT AN OPTION FOR PS-LTE,UK NEC

[179] https://firstnet.gov/,"FirstNetNetwork",[Online].Available:https://firstnet.gov/network,[Accesed:4-August-2021]

[180] Favraud, Romain &Apostolaras, Apostolos &Nikaein, Navid &Korakis, Thanasis. (2016). Toward moving public safety networks. IEEE Communications Magazine. 54. 14-20. 10.1109/MCOM.2016.7432142.

[181] https://firstnet.gov/,“FirstNet enabled location services: Enhancing situational awareness and improving public safety outcomes”,[Online].Available: https://firstnet.gov/newsroom/blog/firstnet-enabled-location-services-enhancing-situational-awareness-and-improving ,[Accesed:5-August-2021]

[182] https://www.samsung.com/,”Solid Foundation Stable and Secure Communications”,[Online].Available:https://www.samsung.com/global/business/networks/solutions/public-safety/,[Accesed:5August-2021]

[183] https://www.sandvine.com/ “Traffic Steering/Diversion Intelligently redirect traffic and better allocate network resources”,[Online].Available: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Solutions%20Briefs/Network%20Optimization/Sandvine_SB_Traffic%20Steering.pdf/,[Accesed:6August-2021]

[184] https://blog.wirelessmoves.com/, “LTE-A Pro for Public Safety Services - Part 3 - The Challenges,[Online].Available: https://blog.wirelessmoves.com/2016/01/lte-a-pro-for-public-safety-services-part-3-the-challenges.html/,[Accesed:7August-2021]

[185] B. Bertenyi, "5G Evolution: What's Next?," in *IEEE Wireless Communications*, vol. 28, no. 1, pp. 4-8, February 2021, doi: 10.1109/MWC.2021.9363048.

[186] https://www.xbase.com/”How can I make my network scalable”,[Online].Available: https://www.xbase.com/2020/01/how-can-i-make-my-network-scalable//,[Accesed:8August-2021]

[187] W. Yu, H. Xu, J. Nguyen, E. Blasch, A. Hematian and W. Gao, "Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions," in *IEEE Access*, vol. 6, pp. 70397-70425, 2018, doi: 10.1109/ACCESS.2018.2879760.

[188] K. Ali, H. Nguyen, P. Shah, Q. Vien, and N. Bhuvanasundaram, “Architecture for Public Safety Network Using D2D Communication,” in IEEE Wireless Communications and Networking Conference, Apr. 2016, pp. 1 – 6.