Review

Toward Intelligent and Resilient Public Safety Communications: A Comprehensive Review of FirstNet, 5G, AI, and Emerging Technologies

Dileesh Chandra Bikkasani *

Posted Date: 23 March 2026

doi: 10.20944/preprints202603.0604.v2

Keywords: first responder communication; FirstNet; 5G NR; network slicing; MCPTT; public safety lte; digital twin; artificial intelligence; iot; satellite communication; 6G; cybersecurity; emergency management

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 March 2026 doi:10.20944/preprints202603.0604.v2

Review

Toward Intelligent and Resilient Public Safety Communications: A Comprehensive Review of FirstNet, 5G, AI, and Emerging Technologies

Dileesh Chandra Bikkasani

University of Bridgeport, Bridgeport, CT, USA; dbikkasa@my.bridgeport.edu

Abstract

Reliable and resilient communication systems are indispensable for first responders, enabling rapid coordination and effective emergency response. However, traditional communication networks frequently encounter congestion, interoperability failures, and infrastructure collapse during large-scale disasters. To address these deficiencies, specialized networks such as the First Responder Network Authority (FirstNet) have been developed, leveraging advancements in Long-Term Evolution (LTE), Fifth-Generation New Radio (5G NR), and priority access mechanisms to enhance reliability and coverage. This comprehensive review examines the technological evolution of first-responder communication systems from legacy Land Mobile Radio (LMR) and Project 25 (P25) systems through modern broadband solutions. We systematically analyze key enablers including network prioritization with Quality of Service (QoS), Priority, and Preemption (QPP); dedicated spectrum allocation on Band 14 (758–768/788–798 MHz); Mission Critical Push-to-Talk (MCPTT), Mission Critical Video (MCVideo), and Mission Critical Data (MCData) standards defined across 3GPP Releases 13–18; network slicing for dedicated emergency virtual networks; and Multi-access Edge Computing (MEC) for ultra-low-latency field processing. Additionally, this study assesses the integration of artificial intelligence and machine learning for predictive network management, digital twin technology for infrastructure resilience simulation, Internet of Things (IoT) sensor ecosystems for enhanced situational awareness, and satellite communication systems, including emerging Low Earth Orbit (LEO) constellations, for connectivity in infrastructure-denied environments. We further examine real-world deployments through case studies encompassing Hurricane Katrina (2005), the September 11 attacks (2001), Hurricane Harvey (2017), the California wildfires (2018–2025), and the 2011 Great East Japan Earthquake, alongside global initiatives including the United Kingdom's Emergency Services Network (ESN), the European Union's Public Protection and Disaster Relief (PPDR) framework, and South Korea's PS-LTE SafeNet. By synthesizing recent advancements across more than 120 scholarly and technical sources, this review provides a forward-looking roadmap addressing Sixth-Generation (6G) networks, terahertz communications, holographic situational awareness, augmented and extended reality for field operations, blockchain-secured data sharing, and cybersecurity frameworks. We conclude with policy recommendations and identify critical research gaps necessary to ensure a seamless, intelligent, and globally interoperable communication infrastructure for first responders.

Keywords: first responder communication; FirstNet; 5G NR; network slicing; MCPTT; public safety lte; digital twin; artificial intelligence; iot; satellite communication; 6G; cybersecurity; emergency management

1. Introduction

Reliable and resilient communication systems form the backbone of effective emergency response, yet traditional networks have repeatedly demonstrated critical vulnerabilities during large-scale disaster scenarios [1]. The September 11, 2001 terrorist attacks starkly revealed these deficiencies: first responders from the Fire Department of New York (FDNY), New York Police Department (NYPD), and Port Authority Police operated on incompatible radio systems with different frequencies and capabilities, directly contributing to the loss of 343 firefighters who were unable to receive evacuation orders [2]. Four years later, Hurricane Katrina in 2005 caused the failure of over 1,000 cell sites, severed fiber-optic cables, and destroyed dozens of central offices across southeastern Louisiana and southern Mississippi, leaving responders without reliable communication during the most critical hours of the disaster [3].

These catastrophic failures catalyzed a fundamental transformation in public safety communications. The 9/11 Commission's recommendations led to the establishment of the First Responder Network Authority (FirstNet) in 2012, a nationwide high-speed broadband network dedicated exclusively to public safety agencies [4]. Operating on Band 14 of the 700 MHz spectrum (758–768/788–798 MHz), FirstNet provides prioritized and preemptive access to ensure that first responders maintain connectivity even during peak network congestion [5]. As of 2025, FirstNet serves more than 6.1 million connections across nearly 30,000 public safety agencies in all 50 states, five territories, the District of Columbia, and tribal lands [6].

In parallel with dedicated network development, the evolution of cellular technology from Fourth-Generation Long-Term Evolution (4G LTE) to Fifth-Generation New Radio (5G NR) has introduced transformative capabilities for emergency communications. The three service categories defined by the Third Generation Partnership Project (3GPP), Ultra-Reliable Low-Latency Communication (URLLC) with latency below 1 millisecond and reliability of 99.999%, Enhanced Mobile Broadband (eMBB) supporting data rates of 10–20 Gbps, and Massive Machine-Type Communication (mMTC) enabling up to one million connected devices per square kilometer, collectively address the diverse requirements of modern emergency response [7,8]. Network slicing technology further enables the creation of dedicated virtual networks within shared physical infrastructure, guaranteeing bandwidth, latency, and reliability parameters specifically tailored for mission-critical applications [9].

The integration of artificial intelligence (AI) and machine learning (ML) into emergency communication systems is revolutionizing network management through predictive analytics, dynamic resource allocation, and real-time anomaly detection [10]. AI-optimized routing for disaster scenarios has demonstrated measurable improvements: 15.5% higher packet delivery ratio, 43% lower delay, 49% increased throughput, and 30% reduced energy consumption compared to traditional approaches [11]. Digital twin technology creates virtual replicas of communication networks, enabling engineers and planners to simulate disaster scenarios, evaluate failover strategies, and test network resilience without affecting live operations [12]. Internet of Things (IoT) ecosystems, comprising wearable biometric sensors, environmental monitoring devices, and aerial drone platforms, provide unprecedented situational awareness, with more than 22,000 first responder agencies in the United States now connected through intelligent safety platforms linking over 600 million IoT devices [13].

Despite these significant advancements, several challenges remain. Interoperability gaps persist as agencies operate on disparate legacy systems including TETRA, P25, and proprietary LMR networks that do not seamlessly integrate [14]. Cybersecurity threats pose a constant risk, with 75% of local public safety organizations reporting cyberattack experiences, yet over 40% lacking cybersecurity planning or procedures [15]. Ensuring reliable connectivity in rural, disaster-affected, and subterranean environments remains a complex challenge requiring ongoing research into alternative communication methods including satellite integration, mesh networking, and device-to-device communication [16].

Looking forward, the anticipated emergence of Sixth-Generation (6G) networks by the 2030s presents promising new capabilities including terahertz (THz) frequency utilization for terabit-per-second data transmission, holographic communication for three-dimensional remote collaboration, AI-native network architectures, and seamless satellite-terrestrial integration [17]. The International

Telecommunication Union (ITU) released the first 6G research timetable in 2020, with commercial deployments planned for 2030 [18].

This paper provides a comprehensive synthesis of recent technological advancements and evaluates persistent challenges in emergency communication. It offers a forward-looking roadmap encompassing technological, policy, and operational dimensions necessary to build a seamless, intelligent, and globally interoperable communication infrastructure for first responders. The remainder of this paper is organized as follows: Section 2 presents the historical background and evolution of public safety communication systems. Section 3 examines the importance of reliable communication through analysis of communication failures and their consequences. Section 4 provides a detailed overview of current first responder communication systems and standards. Section 5 identifies key challenges across interoperability, reliability, security, and scalability dimensions. Section 6 reviews technological innovations including 5G, AI, digital twins, and edge computing. Section 7 presents case studies from major disasters and global deployment initiatives. Section 8 proposes future research directions encompassing 6G, cybersecurity, and ethical considerations. Section 9 concludes with policy recommendations and a summary of contributions.

2. Background and Historical Evolution

2.1. The Imperative for Dedicated Public Safety Communications

Effective communication is the foundation of emergency response, enabling first responders, police, firefighters, emergency medical services (EMS), and other relevant agencies, to coordinate actions, allocate resources, and make real-time decisions in life-critical situations [19]. In natural disasters, terrorist attacks, or large-scale accidents, the ability of emergency personnel to communicate seamlessly can determine survival outcomes for both victims and responders [20]. Emergency response teams must exchange information rapidly to assess threats, provide medical aid, coordinate evacuations, and ensure public safety across multiple jurisdictions [21].

However, traditional communication infrastructures have repeatedly failed during emergencies due to network congestion, interoperability barriers between agencies, physical infrastructure damage, and power system failures [22]. These systemic vulnerabilities have driven the development of dedicated, resilient communication networks specifically engineered for public safety operations.

2.2. From Two-Way Radio to Digital Trunking (1930s–2000s)

The history of first responder communication systems dates to the early twentieth century, when police and fire departments relied on landline telephones and emerging two-way radio technology [23]. During the 1930s and 1940s, radio-based communication gained prominence through Very High Frequency (VHF) and Ultra High Frequency (UHF) systems, enabling emergency personnel to exchange information more efficiently across geographic distances. The development of dedicated public safety radio networks in the 1970s and 1980s marked a significant advancement, though these systems were often fragmented across agencies and lacked standardization [24].

The 1990s and early 2000s saw the introduction of digital trunked radio systems, including Terrestrial Trunked Radio (TETRA) in Europe and Project 25 (P25) in North America, which improved spectrum efficiency and interoperability to some extent [25]. P25, standardized under the Telecommunications Industry Association (TIA) as the TIA-102 series, was developed through joint efforts of the Association of Public Safety Communications Officials (APCO), the National Association of State Telecommunications Directors (NASTD), and federal agencies to enable interoperable Land Mobile Radio (LMR) communications [26]. TETRA, originally conceived in the early 1990s within the framework of the Schengen agreement for European public safety sectors, evolved into the reference technology for mission-critical and business-critical applications worldwide [27].

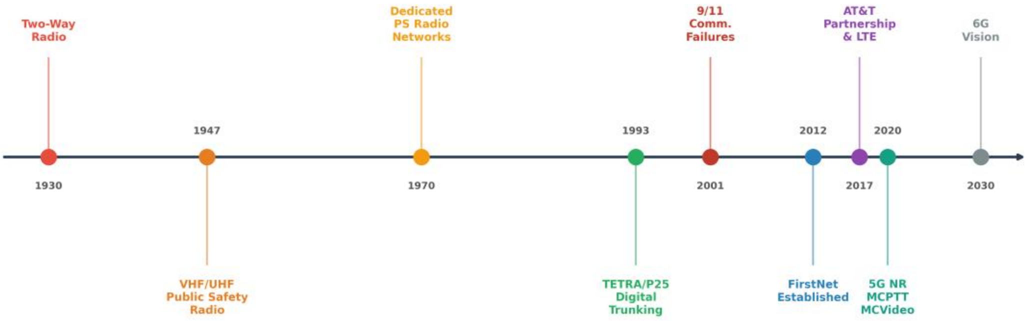

Figure 1. Evolution of First Responder Communication Systems (1930s–2030s).

2.3. The September 11 Catalyst and the Birth of FirstNet

The September 11, 2001 attacks exposed severe, life-threatening limitations in public safety communication when responders from different agencies struggled to communicate due to incompatible radio systems operating on different frequencies with different capabilities [2]. The 9/11 Commission prioritized public safety communications research, leading the National Institute of Standards and Technology (NIST) to establish its Public Safety Communications Research division [28]. After years of policy development and the recommendations of the International Association of Chiefs of Police (IACP), the U.S. Congress established the First Responder Network Authority (FirstNet) in 2012 through the Middle Class Tax Relief and Job Creation Act [4].

FirstNet is structured as an independent authority within the U.S. Department of Commerce, governed by a 15-member Board of Directors that includes three ex officio members (the Secretary of Homeland Security, the Attorney General, and the Director of the Office of Management and Budget) and twelve members appointed by the Secretary of Commerce for their expertise in public safety, technology, network operations, and finance [29]. In March 2017, AT&T was awarded a landmark 25-year public-private partnership contract valued at $6.5 billion from FirstNet over the initial 10 years, with AT&T committing $46.5 billion in total investment over the contract life, leveraging $180 billion in existing infrastructure [30].

2.4. FirstNet Architecture and Spectrum Allocation

FirstNet operates on a dedicated portion of the 700 MHz spectrum designated as Band 14 (758–768 MHz uplink / 788–798 MHz downlink), providing 20 MHz of spectrum with propagation characteristics ideally suited for public safety: excellent building penetration, superior coverage relative to higher frequency bands, and support for High-Powered User Equipment (HPUE) that allows first responders to operate at greater distances from cell towers [5]. The network provides several mission-critical advantages over commercial cellular systems: Quality of Service (QoS) guarantees with deterministic performance, Priority access ensuring first responders receive network resources before commercial users, and Preemption capabilities that remove lower-priority sessions during resource scarcity [31].

The initial five-year network buildout was completed on schedule by 2023 across all 50 states, five territories, the District of Columbia, and tribal lands. As of fiscal year 2024, the network serves 6.1 million connections across more than 28,500 public safety agencies [6]. In February 2024, FirstNet Authority and AT&T announced a 10-year, $8 billion investment plan, including $6.3 billion dedicated to a standalone 5G core for public safety communications and network evolution [32].

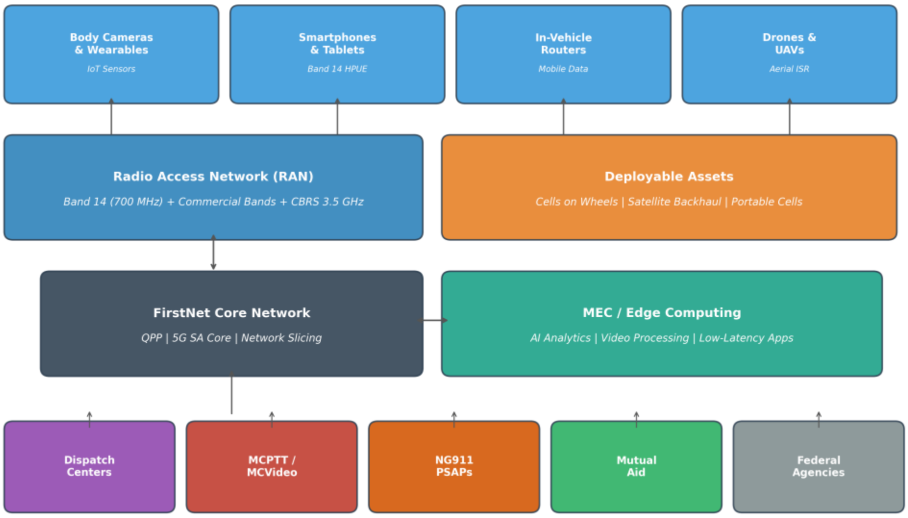

Figure 2. FirstNet Network Architecture.

2.5. Standards Development Ecosystem

The development of public safety communication standards involves multiple organizations working in coordination. The National Public Safety Telecommunications Council (NPSTC), a federation representing public safety telecommunications, plays a central role in defining technical requirements. NPSTC's Broadband Working Group developed requirements for Mission Critical Voice, Local Control, and Priority/QoS that informed FirstNet's design, including the December 2012 Public Safety Broadband Launch Requirements delivered to the FirstNet Board [33]. The SAFECOM program, managed by the Cybersecurity and Infrastructure Security Agency (CISA), serves as an emergency responder-driven initiative to improve inter-jurisdictional and interdisciplinary emergency communications interoperability [34]. At the international level, the European Telecommunications Standards Institute (ETSI), the International Telecommunication Union (ITU), and The Critical Communications Association (TCCA) collaborate on standards for TETRA, 3GPP mission-critical services, and global interoperability frameworks [27].

3. The Critical Role of Reliable Communication in Emergency Response

3.1. Communication as a Force Multiplier

Effective emergency response relies on seamless coordination between multiple agencies to contain threats, deliver medical assistance, and restore normalcy [19]. Police departments require instant updates from dispatch centers to assess threats and manage law enforcement actions. Fire departments depend on immediate situational awareness to deploy resources efficiently with appropriate equipment. Emergency Medical Services must maintain seamless communication with hospitals for patient preparation and care coordination [21]. Modern technologies, including video streaming from body cameras, drone aerial feeds, and IoT sensor data, further enhance situational awareness by providing decision-makers with real-time information from the field [35].

Beyond immediate response, communication plays a crucial role in long-term disaster management and recovery. Following major incidents such as hurricanes, earthquakes, or wildfires, authorities must coordinate large-scale relief operations, deploy emergency shelters, and restore essential services [36]. Government agencies rely on reliable networks to disseminate public safety alerts through systems such as the Wireless Emergency Alerts (WEA) system, which uses cell broadcast technology standardized by 3GPP to deliver geographically-targeted alerts through FEMA's Integrated Public Alert and Warning System (IPAWS) [37].

3.2. Consequences of Communication Failures: Lessons from Major Disasters

Communication failures have produced devastating consequences across multiple disaster scenarios, providing critical lessons for system design and policy development.

September 11, 2001. The attacks on the World Trade Center revealed that the FDNY, NYPD, and Port Authority Police operated on incompatible radio systems. The absence of interoperable standards between different radio manufacturers, frequencies, and jurisdictions prevented life-saving coordination. The Federal Aviation Administration was excluded from the National Military Command Center Air Threat Conference Call due to equipment problems and secure phone number difficulties [2]. These failures directly motivated the creation of FirstNet and NIST's Public Safety Communications Research program [28].

Hurricane Katrina, 2005. The hurricane caused massive infrastructure damage across southeastern Louisiana and southern Mississippi: over 1,000 cell sites were knocked out of service, dozens of central offices were destroyed, and countless miles of outside plant and fiber-optic cable were damaged or severed [3]. Persistent difficulty in designing and implementing communications infrastructure for multi-jurisdictional information exchange, combined with the absence of a unified incident reporting system, led to cascading outages and a chaotic, uncoordinated response [38].

Great East Japan Earthquake and Tsunami, 2011. Approximately 8,000 mobile base stations were immediately disabled, with the number doubling within 24 hours as backup power was exhausted, backup power failure accounted for 85% of mobile communication breakdown [39]. Carriers imposed restrictions reducing 80–90% of fixed-line and 70–95% of mobile traffic to prioritize emergency calls. Critically, almost half of the affected population received no tsunami information or evacuation orders, and 60–70% did not receive revised tsunami height information [39].

Hurricane Harvey, 2017. During the hurricane, 4% of cell sites went out of service initially, with five out-of-service switching centers and 38 operating on backup power. The 911 system received 75,000 calls from Friday night to Monday morning against a normal baseline of 8,000–9,000 calls per day, overwhelming official rescue forces [40]. FirstNet demonstrated its value by providing priority network access that prevented congestion issues common on commercial networks [41].

California Wildfires, 2018–2025. The 2018 Camp Fire destroyed 66 cell sites in Butte County alone, creating communication blackouts during the evacuation of Paradise, California [42]. During the 2020–2021 wildfire seasons, FirstNet improved situational awareness for firefighters through drone-based aerial imaging and sensor data integration, even in areas with damaged infrastructure [43]. However, the January 2025 Los Angeles wildfires exposed continued vulnerabilities: a Wireless Emergency Alert intended for the Kenneth Fire area was mistakenly delivered to the entire Los Angeles County, reaching nearly 10 million people with a false evacuation order, causing panic and information fatigue [44].

3.3. The Trust Dimension

Beyond physical consequences, failures in emergency communication systems erode public trust in authorities [45]. When communities perceive response efforts as slow or inadequate due to poor communication, misinformation and panic can spread, leading to increased chaos. Distrust in emergency services may discourage individuals from following official instructions in future emergencies, creating a negative feedback cycle that further complicates disaster management. The COVID-19 pandemic amplified these trust challenges: inconsistent and incongruent government communications, rapid information evolution with emerging variants, and the over-abundance of both accurate and inaccurate information, termed the "infodemic", collectively eroded public confidence in emergency messaging systems [46].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 March 2026 doi:10.20944/preprints202603.0604.v2

4. Overview of First Responder Communication Systems and Standards

4.1. Legacy Systems: Land Mobile Radio and P25

Land Mobile Radio (LMR) systems have long served as the backbone of first responder communication, providing dedicated, secure, and mission-critical voice communications operating on VHF and UHF frequency bands [47]. These systems enable emergency personnel to communicate over long distances independent of commercial cellular networks. LMR technology remains highly reliable in emergencies and resistant to interference, though it is limited by restricted data transmission capabilities, interoperability challenges between agencies, and coverage gaps in rural areas [48].

Project 25 (P25) standards, published as the TIA-102 series comprising 49 separate parts, represent the North American standard for interoperable LMR systems [26]. P25 supports analog conventional, digital conventional, digital trunked, and mixed-mode configurations. Phase I provides a single voice channel per 12.5 kHz bandwidth, while Phase II introduces the Advanced Multi-Band Excitation (AMBE2+) vocoder enabling compressed bitstreams and two Time Division Multiple Access (TDMA) voice channels within the same 12.5 kHz radio frequency bandwidth, effectively doubling spectral efficiency [49].

Table 1. Comparison of First Responder Communication Technologies.

Technology	Data Rate	Latency	Coverage	Interoperability	Era
LMR/P25	Narrowband (9.6 kbps)	Low (analog)	Wide (VHF/UHF)	Limited (agency-specific)	1970s–Present
TETRA	28.8 kbps	Low	Wide	Moderate (European std)	1995–Present
LTE (Band 14)	Up to 100 Mbps	~10–50 ms	Nationwide (700 MHz)	High (FirstNet QPP)	2017–Present
5G NR (URLLC)	10–20 Gbps peak	<1 ms	Urban/Suburban (sub-6 + mmWave)	Very High (Network Slicing)	2020–Present
6G (Vision)	>1 Tbps	<0.1 ms	Global (Satellite-Integrated)	AI-Native (Autonomous)	~2030

4.2. Modern Broadband Solutions: LTE and FirstNet

The advent of LTE technology revolutionized first responder communication by providing high-speed data transmission and enabling advanced applications such as real-time video streaming, Geographic Information System (GIS) mapping, and automated emergency response systems [50]. FirstNet, operating on dedicated Band 14 spectrum, addresses the limitations of commercial cellular networks through several mechanisms: dedicated network core infrastructure with priority and preemption features; encrypted data transmission with cybersecurity protections; extended coverage in rural and underserved areas through purpose-built sites; and deployable network assets for rapid emergency coverage [5,31].

Performance comparisons between public safety LTE and commercial LTE reveal significant differences in mission-critical scenarios. Public safety LTE achieves end-to-end latency targets below

5 milliseconds for up to 200 active users with deterministic QoS, whereas commercial networks exhibit variable performance during peak periods due to shared resources and best-effort service [51]. FirstNet's QPP (Quality, Priority, and Preemption) framework implements multiple priority levels and the ability to remove lower-priority sessions during resource scarcity, ensuring uninterrupted service for emergency personnel [31].

4.3. Mission Critical Services: MCPTT, MCVideo, and MCData

The 3GPP has standardized a comprehensive framework of Mission Critical (MC) services across multiple releases. Release 13 (2016) introduced the first global MCPTT standard, providing group communication with arbitrated talk permission over LTE networks [52]. Release 14 (2017) expanded the framework to include MCVideo, supporting group and private video calls with H.264 (AVC) mandatory codec support and optional H.265 (HEVC) at resolutions up to 720p, and MCData, enabling messaging, file distribution, and data streaming [53]. Subsequent releases through Release 18 (2024) have introduced enhancements including MC gateway user equipment, ad hoc group communication, and MC services using 5G Multicast and Broadcast Services [54].

These standards are gaining global adoption. South Korea's SafeNet, one of the world's first 3GPP-compliant nationwide public safety networks, provides connectivity to over 330 organizations using Samsung's MCPTT implementation, which supports simultaneous transmission to up to 2,500 user devices per cell through evolved Multimedia Broadcast Multicast Service (eMBMS) [55]. In June 2024, the Global Certification Forum (GCF) began a certification program in collaboration with TCCA for Broadband Mission Critical Services, initially targeting 3GPP Release 14 MCPTT with planned expansion to MCData and MCVideo [56].

4.4. Device-to-Device Communication and Proximity Services

3GPP Release 12 introduced Proximity Services (ProSe), enabling direct device-to-device (D2D) communication without network intermediary support [57]. ProSe provides device discovery, direct group communication, and user equipment-to-network relay capabilities through a sidelink interface with dedicated resource pools. This technology is critically important for first responders operating in areas with degraded or absent cellular coverage.

The evolution continued through Release 16 with the introduction of NR Sidelink (PC5) for direct communication supporting unicast, groupcast, and broadcast modes in both in-coverage and out-of-coverage scenarios [58]. Release 17 introduced NR Proximity Services specifically targeting public safety applications, with NIST releasing simulation models for performance evaluation [59]. NR sidelink offers lower latency, larger payloads, and higher data rates compared to LTE-based D2D communication, with support for Hybrid Automatic Repeat Request (HARQ) operation at the MAC level for enhanced reliability [60].

4.5. IoT Integration and Smart Sensor Ecosystems

The Internet of Things has transformed first-responder communication by integrating smart devices, sensors, and automated systems to enhance situational awareness. Wearable devices, including smart helmets, biometric sensors monitoring heart rate, body temperature, and blood oxygen saturation (SpO2), and body-worn cameras, provide real-time health monitoring and environmental data to ensure responder safety [61]. In the United States, over 22,000 first responder agencies use intelligent safety platforms linking over 600 million IoT devices, from phones and wearables to connected vehicles and home sensors, directly with 911 centers and field responders [13].

Drones assist in aerial surveillance, search and rescue operations, and live video streaming. Cooperative aerial wireless networks composed of small unmanned aerial vehicles (UAVs) are easily deployable, providing on-the-fly communication facilities through wireless access points [62]. Smart sensors deployed in hazardous environments detect toxic gases, structural instability, and extreme

doi:10.20944/preprints202603.0604.v2

temperatures, sending early warnings to emergency personnel through edge computing nodes that ensure low-latency, high-availability operations [63].

4.6. Satellite-Based Communication Systems

In remote or disaster-affected regions where cellular networks and traditional radio systems are unavailable, satellite-based communication systems provide a critical backup. Low Earth Orbit (LEO) constellations have transformed this capability: Starlink has deployed 7,000–8,000 satellites with over 6 million active customers, while OneWeb operates 618–648 satellites in its first-generation constellation [64]. LEO satellites offer 15–20 times lower latency (20–40 ms versus 250–600 ms for Geostationary Earth Orbit systems), 10–50 times higher bandwidth (50–300 Mbps), and 60–70% cost reduction [65].

Practical deployments have validated these advantages: first responders in Washington state reported that Starlink LEO terminals achieved operational status within 5–10 minutes compared to up to one hour for traditional satellite connections [66]. During major California wildfires, portable Starlink kits were deployed to restore emergency communications in areas with no functioning cellular or fiber networks. However, LEO satellite resilience under multi-hazard scenarios remains an active area of research, with studies evaluating constellation performance against earthquakes, floods, and hurricanes [67].

5. Key Challenges in First Responder Communication

5.1. Interoperability

Interoperability remains one of the most persistent challenges in emergency communications. Response agencies, including law enforcement, fire departments, EMS, and federal agencies, often operate on different communication systems with proprietary technologies and frequency bands [68]. Each agency typically utilizes its own set of communication devices, leading to fragmented communication and delayed response times during multi-agency operations. The proliferation of multiple technologies, P25, TETRA, TETRAPOL, DMR, and broadband LTE/5G, has created a complex interworking landscape. Device vendors are responding with multi-bearer terminals combining P25, TETRA, DMR, and 3GPP broadband access, and hybrid network implementations such as dual-mode TETRA-LTE radios are expanding coverage in buildings and areas lacking cellular connectivity [69]. Standardized gateway technologies and nationwide emergency networks like FirstNet aim to bridge these gaps, but the transition from legacy to broadband systems will require decades-long migration paths, with Western and Northern European countries planning TETRA-to-3GPP migration between 2028 and 2031 [70].

5.2. Reliability and Coverage

Communication systems must function under extreme conditions including severe weather, power outages, and large-scale infrastructure destruction. Many rural and remote locations suffer from weak or nonexistent network coverage, with the wireless broadband in public safety market projected to grow from $38.26 billion in 2024 to $111.16 billion by 2029, driven largely by demand for enhanced rural coverage [71]. Natural disasters exacerbate these issues by damaging infrastructure and causing cascading network failures. During large-scale incidents, commercial networks experience traffic surges that cause congestion and call failures; without priority access mechanisms, first responders must compete with public users for bandwidth [72].

Deployable network solutions, including Cells on Wheels (CoWs), satellite terminals, and UAV-based aerial base stations, provide temporary coverage augmentation. FirstNet has deployed over 14,000 miniature cell sites and 135 purpose-built cell sites nationwide, in addition to its deployable asset fleet [6]. However, ensuring seamless handoff between fixed and deployable infrastructure during rapidly evolving incidents remains technically challenging.

5.3. Cybersecurity

With the increasing digitization of emergency communication, protecting sensitive information from cyber threats has become critically important. First responder networks face risks from ransomware attacks, denial-of-service (DoS) disruptions, and unauthorized interception [73]. The transition to Next-Generation 911 (NG911), which enables real-time video and text transmission from the public to Public Safety Answering Points (PSAPs) over IP platforms, expands the cybersecurity attack surface significantly [74]. Despite these growing threats, a SAFECOM nationwide survey found that over 40% of local public safety organizations do not conduct cybersecurity planning or implement cybersecurity procedures [15].

Government agencies are advancing countermeasures through multiple initiatives. CISA has scaled Endpoint Detection and Response deployment to over 60 agencies with 500,000 visible endpoints, blocking 2.62 billion malicious connections within federal civilian networks [75]. The Department of Homeland Security is prototyping capabilities to reduce emergency communications system risk, enhancing mobile authentication of public safety officials, and securing voice and data communications through multi-factor authentication and end-to-end encryption [15].

5.4. Scalability and Spectrum Management

As urban populations grow and climate-related disasters increase in frequency and intensity, first-responder communication networks must scale efficiently. The Citizens Broadband Radio Service (CBRS) at 3.5 GHz (3550–3700 MHz) introduces a three-tier dynamic spectrum sharing framework, Incumbent Users, Priority Access Licensees (PAL), and General Authorized Access (GAA), managed by cloud-based Spectrum Access Systems that enable real-time interference prevention and priority user protection [76]. The California National Guard has conducted trials with rapidly deployable private 5G networks using CBRS spectrum for emergency response teams [76].

Integration of emerging technologies such as 5G network slicing, ultra-reliable low-latency communication (URLLC), edge computing, and carrier aggregation offers new approaches to scaling emergency networks. These advancements enable faster data exchange, real-time decision-making, and dedicated virtual networks isolated from public traffic. However, adoption requires substantial infrastructure investment, policy coordination across jurisdictions, workforce training, and resolution of permitting challenges that can require up to four years for regulatory approval in some jurisdictions [77].

6. Technological Innovations and Solutions

6.1. 5G New Radio for Public Safety

The rollout of 5G NR has introduced a transformative shift in first responder communication through three service categories addressing distinct operational requirements [7]. URLLC provides end-to-end latency below 1 millisecond with reliability of 99.999% (packet error rate of 10^-5 to 10^-7), essential for real-time control of drones, robots, and autonomous vehicles in hazardous environments [78]. eMBB supports high-bandwidth applications with data transfer rates of 10–20 Gbps peak, enabling simultaneous real-time video streaming from multiple body cameras, drone feeds, and surveillance systems [8]. mMTC enables deployment of massive IoT sensor networks with up to one million devices per square kilometer for comprehensive environmental monitoring [7].

The 5G NR architecture introduces several features specifically beneficial for public safety. Mini-slot scheduling enables transmission time intervals as short as 70 microseconds at 30 kHz subcarrier spacing, achieving latency reductions of up to 10 times compared to LTE [78]. NR positioning capabilities provide location accuracy of 20–30 centimeters in specific deployments, critical for indoor rescue operations in high-rise buildings [79]. Operating across both sub-6 GHz (FR1: 410 MHz–7.125 GHz) and millimeter-wave (FR2: 24.25–52.6 GHz) frequency ranges, 5G NR offers deployment flexibility: sub-6 GHz provides superior building penetration and wide-area coverage essential for

doi:10.20944/preprints202603.0604.v2

disaster scenarios, while mmWave delivers ultra-high bandwidth for command post and incident area applications [80].

6.2. Network Slicing for Dedicated Emergency Networks

Network slicing enables a single physical 5G infrastructure to be logically divided into multiple isolated virtual networks, each with specific resource allocation and performance guarantees [9]. For emergency services, dedicated slices provide guaranteed bandwidth allocation, ultra-low latency targets, highest priority traffic handling, and automatic resource reallocation during network congestion. The isolation from commercial traffic ensures that emergency operations are unaffected by public network activity.

Real-world implementations are accelerating: Verizon has deployed its Frontline Network Slice providing coast-to-coast emergency access, T-Mobile launched T-Priority as the first 5G network slice for public safety, and AT&T has integrated network slicing into FirstNet's 5G evolution [81]. As of September 2024, 57 mobile operators globally have launched 5G Standalone (SA) networks, a prerequisite for network slicing, with 88 additional operators planning deployment [82]. Academic research continues to advance dynamic network slicing frameworks, including the DYSOLVE framework for vehicular emergency scenarios and QoS-aware algorithms prioritizing emergency traffic while maintaining non-critical service levels [83].

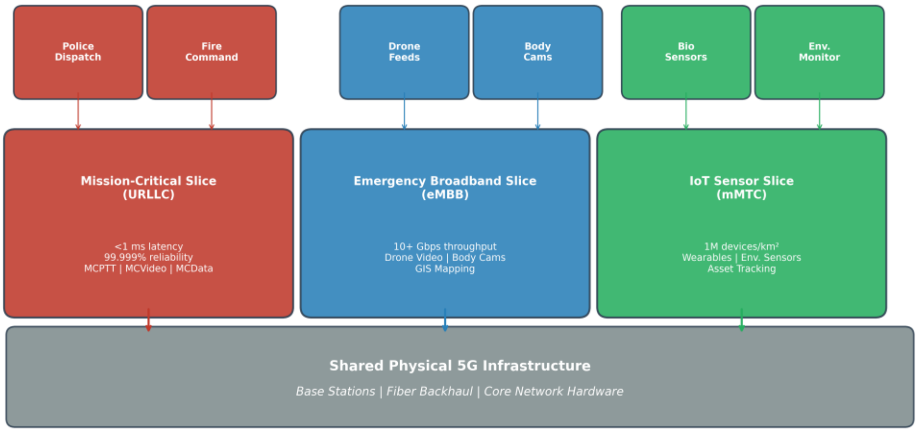

Figure 3. 5G Network Slicing Architecture for Public Safety Communications.

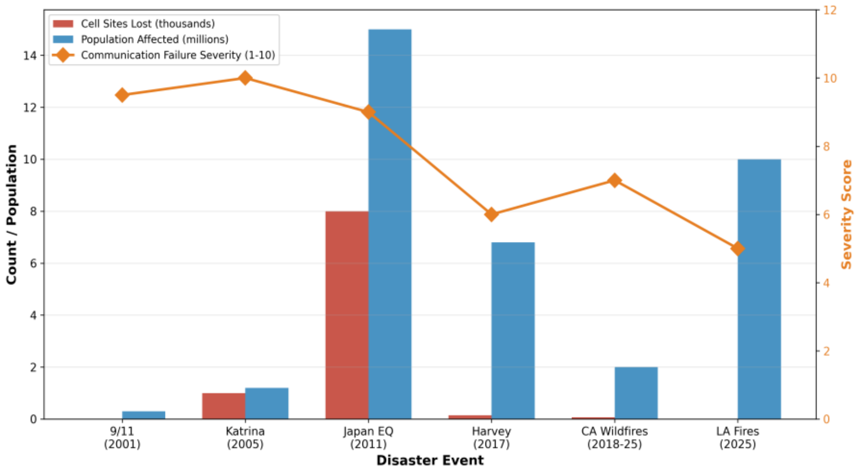

Figure 4. Impact of Communication Failures in Major Disasters.

6.3. Multi-access Edge Computing

Multi-access Edge Computing (MEC) relocates compute-intensive processing from centralized cloud data centers to edge servers positioned at or near base stations, reducing round-trip data processing latency from over 100 milliseconds to single-digit milliseconds [84]. For first responders, this enables real-time video analytics including facial recognition and object detection from surveillance feeds with instant alerts; direct teleoperation of drones and robots in dangerous environments; augmented reality situational awareness overlays; and real-time processing of IoT sensor data from environmental hazard detectors [85].

MEC is particularly valuable in disaster scenarios where backhaul connectivity to centralized data centers may be degraded or severed. Edge computing devices deployed at the scene, including body-worn processors and mobile command post servers, can analyze data locally, sending only essential information to cloud infrastructure and freeing bandwidth for critical voice and video communications [84]. The ETSI Multi-access Edge Computing standards define the architectural framework, with specialized public safety implementations offered by major operators [86].

6.4. AI and Machine Learning for Network Optimization

The integration of AI and ML enhances emergency communication through predictive analytics, dynamic resource allocation, and intelligent decision support. AI-driven models analyze historical disaster data and real-time environmental conditions to forecast network demands and proactively optimize resource positioning [10]. During emergencies, AI-powered systems predict which geographic areas require the most communication capacity based on real-time incident reports, optimize routing for emergency vehicles by analyzing traffic patterns, and dynamically allocate network resources to maintain service quality [87].

AI-powered surveillance and threat detection systems identify potential security threats and alert law enforcement automatically, while natural language processing enables real-time language translation for cross-border emergency coordination [88]. The IEEE Global Communications Conference (GLOBECOM) 2024 hosted a dedicated workshop on Next Generation Intelligent Wireless Emergency Communications, focusing on AI-driven resource allocation, network planning, and QoS provisioning for emergency systems [11].

6.5. Digital Twin Technology for Infrastructure Resilience

Digital twin technology creates comprehensive virtual replicas of real-world communication systems, enabling simulation, analysis, and optimization without affecting operational networks [12]. Network Digital Twins (NDTs) support simulation of diverse network designs, evaluation of operating policies, and modeling of complex fault scenarios under realistic conditions. For public safety, digital twins enable testing network resilience by simulating disasters such as earthquakes and power outages; identifying weak coverage areas and optimizing infrastructure placement for additional cell towers or satellite stations; modeling and evaluating cybersecurity threats, including denial of service, malware, and intrusion scenarios, in isolated virtual environments; and providing immersive training environments for first responders through virtual disaster scenarios [89].

Research in 2025 has demonstrated opportunities for integrating digital twin platforms with 6G network architectures through federated learning frameworks that improve responsiveness and efficiency of resource management in edge-enabled networks [90]. The IETF has developed draft standards for Network Digital Twin Architecture supporting edge-cloud continuum applications [91].

6.6. Software-Defined Networking and Network Function Virtualization

Software-Defined Networking (SDN) and Network Function Virtualization (NFV) enable flexible, programmable, and rapidly reconfigurable network architectures for emergency communications [92]. SDN separates the control plane from the data plane, allowing centralized, intelligent management of network routing and traffic prioritization. NFV virtualizes network functions traditionally implemented in dedicated hardware, enabling rapid deployment and scaling of emergency services infrastructure. Together, these technologies provide simplified network deployment, reduced capital and operating costs, greater agility in responding to emergency demands, and enhanced resilience through automated failover [93].

For public safety, SDN's control plane allows dynamic routing of mission-critical traffic with highest priority, while NFV enables rapid provisioning of network functions when traditional infrastructure is damaged. The combination supports AI-driven optimization of emergency network resources and rapid network reconfiguration during evolving disaster scenarios [92].

6.7. Emerging Technologies: 6G, Terahertz, and Beyond

While 6G remains in the research phase with first commercial deployments planned for 2030, it promises capabilities that could further transform emergency communications [17]. Terahertz communications (220–330 GHz and beyond) enable ultra-high-speed data rates exceeding one terabit per second, though with limited propagation range requiring line-of-sight conditions [94]. The FCC offers experimental licenses for frequencies from 95 GHz to 3 THz, with 21.2 GHz of spectrum available for unlicensed devices in the 0.1–0.3 THz range [95]. Holographic communication may support three-dimensional video conferencing, enabling lifelike remote collaboration between responders, medical personnel, and emergency coordinators [96]. AI-native network architectures will continuously optimize communication parameters based on environmental conditions, ensuring seamless connectivity in dynamic emergency scenarios. Satellite-integrated 6G networks promise uninterrupted connectivity in the most remote or devastated areas through seamless terrestrial-non-terrestrial network integration [17].

7. Case Studies and Global Initiatives

7.1. FirstNet Deployment Impact

FirstNet has demonstrated measurable operational benefits across multiple emergency scenarios. During Hurricane Harvey in 2017, FirstNet ensured uninterrupted communication between police, fire, and EMS in Texas by providing priority network access, preventing the congestion that overwhelmed commercial networks when 911 call volumes increased nearly tenfold [40,41]. During the California wildfire seasons from 2020 onward, FirstNet improved firefighter situational awareness through drone-based aerial imaging, sensor data integration, and robust voice and data services even in areas with severely damaged infrastructure [43]. At major public events such as the 2019 Boston Marathon, FirstNet supported secure communication and crowd monitoring, enabling law enforcement to coordinate responses efficiently [97].

The network continues to expand: as of 2025, FirstNet has deployed 1,000 new Band 14 cell sites, more than 14,000 miniature cell sites, and 135 purpose-built cell sites providing critical facility coverage to public safety agencies at no cost [6]. The fiscal year 2025 budget allocates $684 million, including $534 million dedicated to network investments [32].

7.2. Global Public Safety Network Initiatives

Table 2. Global Public Safety Network Initiatives.

Country/Region	Network	Technology	Status (2025)	Spectrum
United States	FirstNet	LTE/5G (Band 14)	6.1M connections, 30,000 agencies	700 MHz

United Kingdom	ESN	4G LTE	Delayed to 2029, £14B total cost	800 MHz
South Korea	PS-LTE SafeNet	LTE (MCPTT)	Operational, 330+ agencies	700 MHz
European Union	PPDR 5G	5G / TETRA migration	Pilot deployments, 2028–2031 migration	Various
Global Legacy	P25/TETRA/DMR	Digital LMR	Active, declining after 2030	VHF/UHF

United Kingdom: Emergency Services Network (ESN). The ESN is designed to replace the aging TETRA-based Airwave system with an LTE-based solution. In December 2024, BT/EE was awarded a £1.29 billion contract to extend the 4G Emergency Services Network for seven years, with IBM announced as responsible for design, build, and system integration [98]. The project involves 20,840 new and upgraded sites including 292 government-built masts for rural Extended Area Service coverage. However, the project has faced significant delays, the original 2019 completion target has been pushed to 2029, and the total predicted cost has doubled from £6.2 billion to £14 billion [99].

European Union: Public Protection and Disaster Relief (PPDR). The EU's PPDR framework focuses on cross-border emergency communication through dedicated 5G-based disaster-resilient mobile networks for police, border guards, and ambulance services [100]. Specific deployments include a Hungary-Ukraine border 5G PPDR network and the PPDR Transformation Center project specifying interoperable, secure communication architectures. The EU has also mandated public warning systems through the Electronic Communications Code Directive, requiring all member states to implement cell broadcast-based EU-Alert systems, a requirement several states are still completing as of 2025 [101].

South Korea: PS-LTE SafeNet. South Korea's SafeNet operates on 700 MHz spectrum as one of the world's first 3GPP-compliant nationwide public safety networks, serving over 330 organizations with MCPTT, group calls, device-to-device communications, and terminal location services [55]. The network is interconnected with LTE-Maritime and LTE-Railway networks in the same spectrum band, ensuring interoperability across public safety domains.

Interoperability Standards Migration. Globally, narrowband networks based on TETRA, TETRAPOL, and DMR are expected to decline after 2030, with 5G broadband critical communications networks becoming the primary infrastructure. Western and Northern European countries, including the UK, France, Finland, and Sweden, are planning migration from TETRA/TETRAPOL to nationwide mission-critical 3GPP networks between 2028 and 2031 [70]. Multi-bearer interoperability solutions from vendors including Motorola Solutions, L3Harris, and Airbus are providing transitional connectivity [69].

7.3. Lessons from Communication System Failures

Analysis of communication failures across major disasters reveals recurring patterns and systemic vulnerabilities. Infrastructure dependency remains a critical weakness: backup power failure accounted for 85% of mobile communication breakdown during the 2011 Great East Japan Earthquake [39], while physical infrastructure destruction caused cascading failures during Hurricane Katrina [3]. Alert system design requires careful geographic targeting: the 2025 Los Angeles Kenneth Fire false alert reached nearly 10 million people due to a targeting error, causing panic and alert fatigue [44]. Interoperability deficiencies persist across jurisdictions, with multiple unconnected communication platforms causing 20–30 minute decision communication delays during the 2025 Los Angeles wildfires [44]. These case studies collectively underscore the necessity of hardened infrastructure, geographic redundancy, standardized protocols, satellite backups, and continuous investment in resilient network architectures.

8. Future Research Directions

8.1. 6G Networks and Terahertz Communication

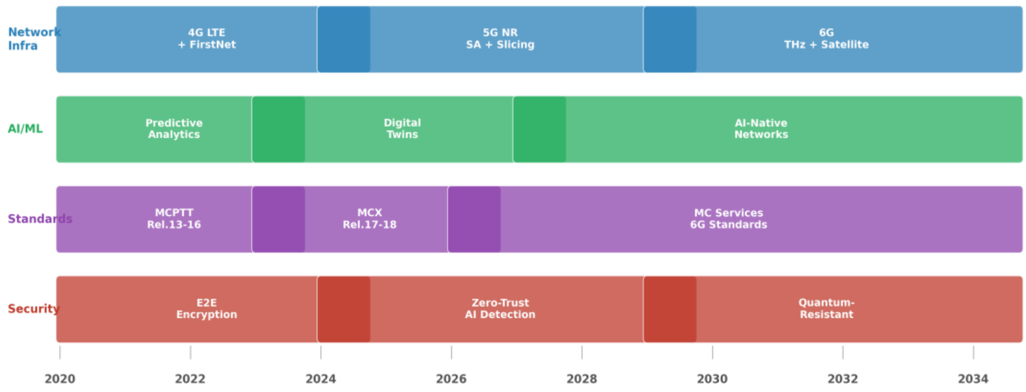

Figure 5. Technology Roadmap for Public Safety Communications (2020–2035).

The ITU released the first 6G research timetable in February 2020, with commercial deployments targeted for 2030 [18]. Key research priorities for public safety include terahertz frequency characterization for emergency environments, including indoor propagation through stairwells and collapsed structures where existing models show significant near-field effects and path loss challenges [102]; holographic communication systems requiring beyond 10 GHz of spectrum for professional high-resolution applications [94]; AI-native network architectures providing autonomous optimization for dynamic emergency scenarios; and satellite-integrated 6G networks ensuring seamless terrestrial-non-terrestrial connectivity [17]. Research challenges include the limited propagation range of THz signals, atmospheric absorption, and human body shadowing effects that reduce signal strength in indoor emergency scenarios [103].

8.2. Augmented and Extended Reality for Field Operations

Augmented reality (AR) and extended reality (XR) technologies are increasingly being integrated into public safety operations. A scoping literature review analyzing publications through April 2025 identified 90 relevant studies demonstrating significant growth in AR user interface integration across EMS, firefighting, and law enforcement applications [104]. Federal investment is accelerating: Carnegie Mellon University received $1.27 million through NIST’s Public Safety Innovation Accelerator Program for developing ruggedized AR interfaces with adaptive head-up displays, haptic interfaces, intelligent thermography, and gesture control for extreme environments [105]. AR systems such as RespondEye enable hands-free telehealth for field EMTs through live see-what-I-see video connections with emergency department physicians [106]. AR interfaces for adverse-visibility conditions have been validated through pilot testing with first responders in mountain rescue, earthquake, and tunnel training scenarios [107].

doi:10.20944/preprints202603.0604.v2

8.3. Blockchain for Secure Emergency Data Sharing

Blockchain technology offers potential for secure and trusted emergency data management through decentralized storage, tamper-proof audit trails, and automated access control via smart contracts [108]. Smart contracts can automatically share specific sensor data with authorized emergency response teams during crisis events while restricting access to non-critical and personal information. Hierarchical blockchain models enable information sharing among emergency response departments using distributed trust mechanisms [109]. A comprehensive bibliometric analysis examining 248 research articles from 2017 to 2024 identified seven major research clusters around blockchain's role in improving transparency, efficiency, and trust in emergency operations [110].

8.4. Cybersecurity Frameworks and Ethical Considerations

Future research must address the expanding attack surface of increasingly digital emergency communications. The transition to NG911 IP platforms, widespread IoT deployment, and cloud-native network architectures create new vulnerability vectors including supply chain compromises, technology espionage, and cross-domain attack propagation in cyber-physical systems [73,74]. Research priorities include privacy-preserving AI models for emergency analytics, zero-trust security architectures for public safety networks, quantum-resistant encryption for long-term communication security, and explainable AI frameworks that maintain public trust in automated emergency decision-making [111].

8.5. Global Interoperability and Resilient Infrastructure

Global emergencies frequently require cross-border coordination, but fragmented communication systems present significant interoperability challenges. Future research should explore AI-based real-time language translation for international emergency coordination, standardized communication protocols enabling seamless network cooperation, and resilient communication systems for extreme environments including collapsed buildings, underground tunnels, and underwater operations [112]. Mesh networking for underground communication, underwater acoustic communication, AI-driven disaster resilience models, and energy-efficient systems are all active areas of investigation [113].

9. Conclusion

Effective communication is the lifeline of emergency response, enabling coordination, real-time information sharing, and rapid decision-making that directly determines survival outcomes. This comprehensive review has examined the full arc of first responder communication evolution, from early two-way radio systems through P25 and TETRA standards, LTE-based broadband solutions including FirstNet, and the ongoing 5G NR transformation providing URLLC, network slicing, and mission-critical services standardization across 3GPP Releases 13–18.

The evidence synthesized from more than 120 scholarly and technical sources demonstrates that modern technologies, 5G network slicing, AI-driven analytics, IoT sensor ecosystems, digital twin simulation, MEC, and LEO satellite constellations, are collectively transforming public safety communication by enabling faster response times, more intelligent decision-making, and resilient network architectures. Case studies from FirstNet's operational impact across U.S. disasters and global initiatives including the UK's ESN, the EU's PPDR framework, and South Korea's PS-LTE SafeNet confirm that dedicated broadband networks with priority access mechanisms substantially improve emergency coordination outcomes.

However, challenges remain across four dimensions. First, interoperability gaps between legacy LMR systems and broadband networks require decade-long migration strategies supported by multi-bearer terminal technologies and standardized gateway solutions. Second, cybersecurity threats demand comprehensive frameworks encompassing end-to-end encryption, multi-factor authentication, AI-driven anomaly detection, and workforce training, particularly as NG911 and IoT integration expand the attack surface. Third, reliable coverage in rural, remote, and extreme environments necessitates continued investment in deployable assets, satellite integration, mesh networking, and device-to-device communication capabilities. Fourth, scalability challenges require dynamic spectrum management through frameworks such as CBRS and network slicing to accommodate growing capacity demands.

Looking forward, 6G networks, terahertz communications, holographic situational awareness, augmented reality interfaces, blockchain-secured data sharing, and AI-native architectures will further expand the capabilities available to first responders. Realizing this vision will require coordinated international efforts, standardized protocols, robust regulatory frameworks addressing data privacy and security, sustained infrastructure investment, and workforce development programs that ensure first responders can fully leverage emerging capabilities.

By addressing these interconnected technical, policy, and operational challenges, emergency communication networks will evolve into intelligent, adaptive, and globally interconnected systems that ensure first responders always have secure, reliable, and efficient communication, regardless of the crisis they face.

References

1. G. Deepak et al., “An overview of post-disaster emergency communication systems in the future networks,” IEEE Wireless Communications, vol. 26, no. 6, pp. 132–139, 2019.
2. “Communication during the September 11 attacks,” NIST, 2011. [Online]. Available: https://www.nist.gov/blogs/taking-measure/how-911-changed-me-and-first-responder-communications
3. “Hurricane Katrina: Communications & Infrastructure Impacts,” Defense Technical Information Center, DTIC Report ADA575202, 2005.
4. L. K. Moore, “The first responder network (FirstNet) and next-generation communications for public safety: Issues for congress,” Congressional Research Service, Report R45179, 2016.
5. “FirstNet Band 14 Coverage,” First Responder Network Authority, 2025. [Online]. Available: https://www.firstnet.com/coverage/band-14.html
6. “FirstNet Authority Financial Report, Fiscal Year 2024,” FirstNet Authority, 2024.
7. M. Nuriev et al., “The 5G revolution transforming connectivity and powering innovations,” in E3S Web of Conferences, 2024, EDP Sciences.
8. “Understanding important 5G concepts: What are eMBB, URLLC and mMTC?,” Verizon, 2024.
9. “Public safety mobile broadband system: From shared network to logically dedicated approach leveraging 5G network slicing,” IEEE Xplore, Document 9129819, 2020.
10. M. El-Hajj, “Enhancing communication networks in the new era with artificial intelligence: Techniques, applications, and future directions,” Network, vol. 5, no. 1, p. 1, 2025.
11. “AI-Enabled Emergency Communication Networks,” European Modern Studies Journal, 2024.
12. E. Brucherseifer et al., “Digital twin conceptual framework for improving critical infrastructure resilience,” at-Automatisierungstechnik, vol. 69, no. 12, pp. 1062–1080, 2021.
13. “RapidSOS Intelligent Safety Platform,” RapidSOS, 2024. [Online]. Available: https://www.rapidsos.com
14. S. Daousis et al., “Overview of protocols and standards for wireless sensor networks in critical infrastructures,” Future Internet, vol. 16, no. 1, p. 33, 2024.
15. “Public Safety Cybersecurity,” Cybersecurity and Infrastructure Security Agency (CISA), 2025. [Online]. Available: https://www.cisa.gov/public-safety-cybersecurity
16. M. Matracia et al., “Post-disaster communications: Enabling technologies, architectures, and open challenges,” IEEE Open Journal of the Communications Society, vol. 3, pp. 1177–1205, 2022.
17. R. Kumar et al., “From efficiency to sustainability: Exploring the potential of 6G for a greener future,” Sustainability, vol. 15, no. 23, p. 16387, 2023.
18. International Telecommunication Union, “6G Research Timetable,” ITU, 2020.
19. F. Mwandembo, “Navigating the storm: Effective crisis communication strategies,” International Journal of Innovative Science and Research Technology, pp. 2685–2697, 2024.

20. A. Carreras-Coch et al., "Communication technologies in emergency situations," Electronics, vol. 11, no. 7, p. 1155, 2022.
21. S. E. Mahon and J. J. Rifino, "Role of emergency medical services in disaster management and preparedness," in Ciottone's Disaster Medicine, Elsevier, 2024, pp. 12–18.
22. K. Ali et al., "Disaster management communication networks: Challenges and architecture design," in 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), IEEE, 2015.
23. H. H. Perritt Jr., "The Internet adopts two-way radio," Hastings Science & Technology Law Journal, vol. 10, p. 147, 2019.
24. S. Goldsmith and W. D. Eggers, Governing by Network: The New Shape of the Public Sector. Rowman & Littlefield, 2005.
25. C. M. Hainbuchner, "Technology acceptance of complex products and systems: The case of Terrestrial Trunked Radio (TETRA)," 2005.
26. "Project 25 (P25)," Cybersecurity and Infrastructure Security Agency, 2024. [Online]. Available: https://www.cisa.gov/safecom/project-25
27. "TETRA Home," The Critical Communications Association, 2025. [Online]. Available: https://tcca.info/tetra/home/
28. "How 9/11 Changed Me, and First Responder Communications," National Institute of Standards and Technology, 2021.
29. "FirstNet Authority About," First Responder Network Authority, 2025. [Online]. Available: https://firstnet.gov/about
30. U.S. Government Accountability Office, "Public-Safety Broadband Network," GAO Report GAO-22-104915, 2022.
31. "Quality, Priority, and Preemption," National Public Safety Telecommunications Council, 2020.
32. "FirstNet Authority Board Approves FY25 Budget," FirstNet Authority, 2024.
33. "NPSTC Public Safety Broadband Launch Requirements," National Public Safety Telecommunications Council, December 2012.
34. "SAFECOM Program," Cybersecurity and Infrastructure Security Agency, 2025. [Online]. Available: https://www.cisa.gov/safecom
35. R. Damaševičius, N. Bacanin, and S. Misra, "From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management," Journal of Sensor and Actuator Networks, vol. 12, no. 3, p. 41, 2023.
36. W. Liu and L. Ni, "Relationship matters: How government organization–public relationship impacts disaster recovery outcomes among multiethnic communities," Public Relations Review, vol. 47, no. 3, p. 102047, 2021.
37. "Wireless Emergency Alerts," Federal Communications Commission, 2025. [Online]. Available: https://www.fcc.gov/public-safety-and-homeland-security/alerting/general/wireless
38. "Failure of Initiative Report: Communications," U.S. House Select Bipartisan Committee, 2006.
39. "Communication Problems After Great East Japan Earthquake of 2011," PubMed Central, PMC4301195, 2015.
40. D. J. Barnett et al., "An analysis of after action reports from Texas hurricanes in 2005 and 2017," Journal of Public Health Management and Practice, vol. 27, no. 2, pp. E71–E78, 2021.
41. "FirstNet in 2024: Year of Growth," FirstNet Authority, 2024.
42. "California wildfires highlighted failures of emergency notification system," GovTech, 2019.
43. A. J. Burns et al., "High altitude platform system (HAPS) communication support for wildland firefighting," 2023.
44. "Lessons from Kenneth Fire False Alerts," U.S. House of Representatives Independent Report, May 2025.
45. H. T. Otal, E. Stern, and M. A. Canbaz, "LLM-assisted crisis management: Building advanced LLM platforms for effective emergency response and public collaboration," in 2024 IEEE Conference on Artificial Intelligence (CAI), IEEE, 2024.

46. "Learning from COVID-19: Government leaders' perspectives on effective risk communication," BMC Globalization and Health, vol. 19, 2023.
47. G. Niringiye, I. N. Oteyo, and T. Bulega, "Spectrum sensing for cognitive VHF land mobile radio communication networks using energy sensing techniques," in 2021 IEEE AFRICON, IEEE, 2021.
48. Q. Wang et al., "An overview of emergency communication networks," Remote Sensing, vol. 15, no. 6, p. 1595, 2023.
49. "P25: The Proven Standard," L3Harris Technologies, 2024.
50. D. V. C. Freire, "Mission-critical communications from LMR to 5G: A technology assessment approach for smart city scenarios," Universidade NOVA de Lisboa, 2023.
51. "Commercial vs. Private vs. Public Safety LTE," Tait Radio Academy, 2024. [Online]. Available: https://www.taitradioacademy.com
52. "Mission Critical Services in 3GPP," 3GPP, 2024. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/mc-services
53. "ETSI TS 122 179 v16.5.0: MCPTT Specifications," European Telecommunications Standards Institute, 2020.
54. "Mission-critical services in 4G/5G and beyond: Standardization, challenges, future perspectives," Sensors, vol. 25, no. 16, p. 5156, MDPI, 2025.
55. "First 3GPP-compliant public safety network with MCPTT launches in South Korea," Computer Weekly, 2020.
56. "How Broadband Mission Critical Device Certification is Being Led by GCF and TCCA," Global Certification Forum, 2024.
57. "Recent advances in 3GPP Rel-12 standardization related to D2D and public safety communications," arXiv:1505.07140, 2015.
58. "V2X in 3GPP standardization: NR sidelink in Rel-16 and beyond," arXiv:2104.11135, 2021.
59. "NIST IR 8372: Study of 5G New Radio (NR) support for direct mode communications," NIST, doi: 10.6028/NIST.IR.8372, 2021.
60. "How 5G sidelink benefits public safety and critical communications," Qualcomm, 2023.
61. "Wearable Sensors for Service Members and First Responders," National Academies of Sciences, Engineering, and Medicine, 2023.
62. N. Papyan et al., "AI-based drone assisted human rescue in disaster environments: Challenges and opportunities," Pattern Recognition and Image Analysis, vol. 34, no. 1, pp. 169–186, 2024.
63. J. Lyu et al., "Intelligent-technology-empowered active emergency command strategy for urban hazardous chemical disaster management," Sustainability, vol. 15, no. 19, p. 14369, 2023.
64. "The impact of LEO satellites on public safety communications," IP Access International, 2024.
65. "Assessing LEO satellite networks for national emergency failover," ACM IMC, 2025.
66. "Can LEO satellites enhance the resilience of Internet to multi-hazard risks?," University of Oregon, PAM 2024.
67. "LEO satellite network resilience analysis: A focus on critical satellites," ACM Digital Library, doi: 10.1145/3697253.3697267, 2024.
68. M. J. DeVito, E. Wood, and T. Frazier, "Standardization and interoperability of small unmanned aircraft systems (sUAS) for disaster management," Journal of Homeland Security and Emergency Management, vol. 19, no. 2, pp. 175–203, 2022.
69. "Public Safety LTE & 5G Market," SNS Telecom & IT, 2025.
70. "An update of public-safety LTE deployment efforts around Europe," RR Media Group, 2024.
71. "Wireless Broadband in Public Safety Market Report," Globe Newswire, April 2025.
72. S. Debnath et al., "A comprehensive survey of emergency communication network and management," Wireless Personal Communications, vol. 124, no. 2, pp. 1375–1421, 2022.
73. J. Yoon et al., "Evaluating the readiness of cyber first responders responsible for critical infrastructure protection," International Journal of Critical Infrastructure Protection, vol. 13, pp. 19–27, 2016.
74. "Cybersecurity Best Practices for Next-Gen 911," IEEE Public Safety Technology, 2024.
75. "Building Resilience: Multifactor Authentication in Public Safety Communications," CISA, 2025.

76. “The innovative spectrum sharing framework connecting Americans,” National Telecommunications and Information Administration, 2023.
77. “Bridging the Digital Divide: Navigating the Challenges of Rural Broadband Deployment,” APCO International, 2024.
78. “Ultra-reliable and low-latency communications in 5G downlink: Physical layer aspects,” IEEE Xplore, Document 8403963, 2018.
79. “Toward 5G Advanced: Overview of 3GPP Releases 17 and 18,” Ericsson Technology Review, 2023.
80. “5G mmWave vs. Sub-6: A comparative study,” NYBSys, 2024.
81. “5G for first responders and the benefits of network slicing,” Verizon Business, 2024.
82. “5G network slicing progress report with a look ahead to 2025,” IEEE ComSoc Technology Blog, December 2024.
83. “Evaluation of multi-operator dynamic 5G network slicing for vehicular emergency,” IFIP Networking, 2020.
84. “How 5G and multi-access edge computing can optimize public safety,” StateTech Magazine, 2019.
85. “How does 5G enhance mission-critical communication?,” IEEE Public Safety Technology, 2024.
86. “Multi-access Edge Computing,” European Telecommunications Standards Institute, 2024.
87. “How AI and predictive analytics will shape EMS, fire, and healthcare in 2026,” MedCity News, February 2026.
88. D. Bhumichai et al., “The convergence of artificial intelligence and blockchain: The state of play and the road ahead,” Information, vol. 15, no. 5, p. 268, 2024.
89. “A new era for digital twins: Progress and industry adoption,” Taylor & Francis, 2025.
90. “Network digital twin for 6G and beyond,” arXiv:2506.01609, 2025.
91. “IETF draft: Network Digital Twin Architecture for Edge-Cloud Continuum,” Internet Engineering Task Force, 2025.
92. “Next generation emergency networks,” Nemergent Solutions, 2024.
93. “SDN and NFV: A New Dimension to Virtualization,” World Scientific Series, 2022.
94. “6G spectrum: Future mobile life beyond 2030,” Ericsson White Paper, 2024.
95. “Federal Communications Commission Technological Advisory Council 6G Working Group Report,” FCC, 2025.
96. A. V. Shvetsov and S. H. Alsamhi, “When holographic communication meets metaverse: Applications, challenges and future trends,” IEEE Access, 2024.
97. N. LaLone, P. O. Dugas, and B. Semaan, “The crisis of designing for disaster: How to help emergency management during the technology crisis we created,” in Proceedings of the International ISCRAM Conference, 2023.
98. “BT and EE extend government’s 4G Emergency Services Network for 7 years,” ISPreview UK, December 2024.
99. “Emergency Services Network: Overview,” UK Government, GOV.UK, 2025.
100. “5G-based Public Protection and Disaster Relief (PPDR 5G),” European Commission Digital Strategy, 2024.
101. “EU-Alert,” European Electronic Communications Code Directive, 2018.
102. “Path loss model for indoor emergency stairwell environment at millimeter wave band for 5G network,” ResearchGate, 2018.
103. “Propagation path loss prediction modelling in enclosed environments for 5G networks,” PubMed Central, PMC9672330, 2022.
104. “Augmented reality user interfaces for first responders: A scoping literature review,” arXiv:2506.09236, 2025.
105. “Public Safety Innovation Accelerator Program: Augmented Reality,” NIST, 2021.
106. “RespondEye: AR solutions for first responders,” RespondEye, 2024.
107. “Augmented reality interface for adverse-visibility conditions validated by first responders in rescue training scenarios,” Electronics, vol. 13, no. 18, p. 3739, MDPI, 2024.
108. “Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks,” Sensors, vol. 23, no. 2, p. 969, MDPI, 2023.

109. "Blockchain for public safety: A survey of techniques and applications," Blockchain: Research and Applications, Elsevier, 2023.
110. "Application of blockchain technology in emergency management: A bibliometric analysis," Applied Sciences, vol. 15, no. 10, p. 5405, MDPI, 2025.
111. F. Neto, J. Granjal, and V. Pereira, "A survey on security approaches on PPDR systems toward 5G and beyond," IEEE Access, vol. 10, pp. 117118–117140, 2022.
112. K. Ali et al., "Review and implementation of resilient public safety networks: 5G, IoT, and emerging technologies," IEEE Network, vol. 35, no. 2, pp. 18–25, 2021.
113. K. Shafique et al., "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," IEEE Access, vol. 8, pp. 23022–23040, 2020.
114. G. del Campo et al., "Virtual reality and internet of things based digital twin for smart city cross-domain interoperability," Applied Sciences, vol. 14, no. 7, p. 2747, 2024.
115. G. Pocovi et al., "Achieving ultra-reliable low-latency communications: Challenges and envisioned system enhancements," IEEE Network, vol. 32, no. 2, pp. 8–15, 2018.
116. J. M. Franklin et al., "Security analysis of first responder mobile and wearable devices," NIST, 2019.
117. J. Li et al., "Toward providing connectivity when and where it counts: An overview of deployable 5G networks," IEEE Communications Standards Magazine, vol. 6, no. 4, pp. 56–64, 2023.
118. A. Yarali, Public Safety Networks from LTE to 5G. John Wiley & Sons, 2020.
119. L. G. Canton, Emergency Management: Concepts and Strategies for Effective Programs. John Wiley & Sons, 2019.
120. K. Carlberg, E. W. Burger, and R. P. Jover, "Dynamic 5G network slicing for first responders," in 2019 Principles, Systems and Applications of IP Telecommunications (IPTComm), IEEE, 2019.
121. Y. Wang et al., "Digital twin approach for enhancing urban resilience: A cycle between virtual space and the real world," Resilient Cities and Structures, vol. 3, no. 2, pp. 34–45, 2024.
122. A. Khan, S. Gupta, and S. K. Gupta, "Emerging UAV technology for disaster detection, mitigation, response, and preparedness," Journal of Field Robotics, vol. 39, no. 6, pp. 905–955, 2022.
123. K. Lorincz et al., "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Computing, vol. 3, no. 4, pp. 16–23, 2004.
124. A. Basnawi, "Addressing challenges in EMS department operations: A comprehensive analysis of key issues and solution," Emergency Care and Medicine, vol. 1, no. 1, pp. 11–23, 2023.
125. F. Kagai et al., "Rapidly deployable satellite-based emergency communications infrastructure," IEEE Access, 2024.
126. V. S. Rajkumar et al., "Cyber attacks on power grids: Causes and propagation of cascading failures," IEEE Access, vol. 11, pp. 103154–103176, 2023.
127. O. I. Poyraz et al., "Cyber assets at risk: Monetary impact of US personally identifiable information mega data breaches," The Geneva Papers on Risk and Insurance, vol. 45, pp. 616–638, 2020.
128. S. A. Betts, "The Internet of Things (IoT) in disaster response," Naval Postgraduate School, Monterey, CA, 2022.
129. J. R. Munavalli, R. R. Deshpande, and J. M. Oli, "AI techniques for 6G applications," in Development of 6G Networks and Technology, 2024, pp. 29–55.
130. "Next-generation wireless communication technologies for improved disaster response and management," ETRI Journal, 2025.