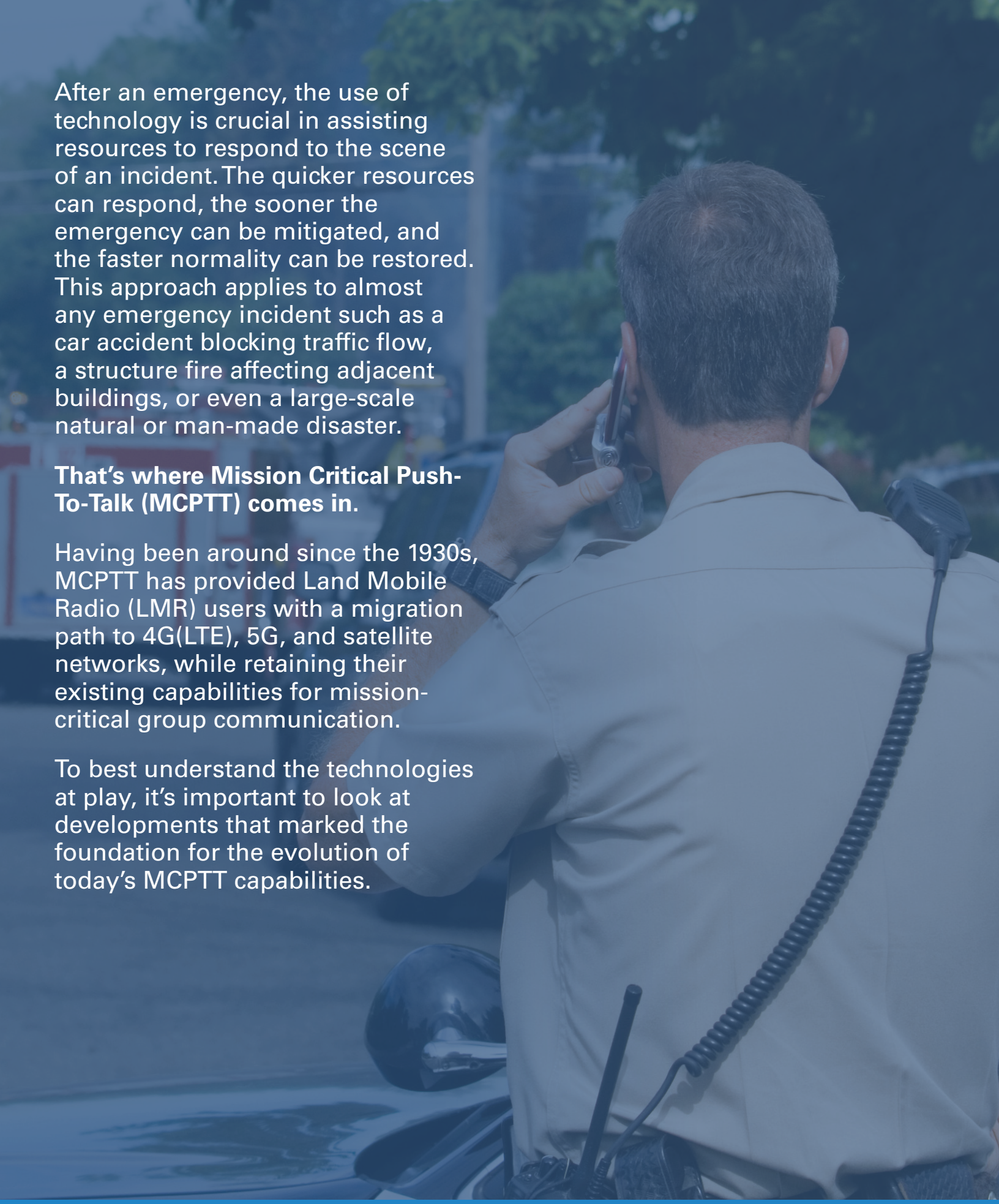
NETWORK INNOVATIONS
Succeed. Anywhere.

WHITE PAPER

Public Safety Interoperability

The Roadmap to Success with Mission Critical Push-To-Talk

networkinv.com

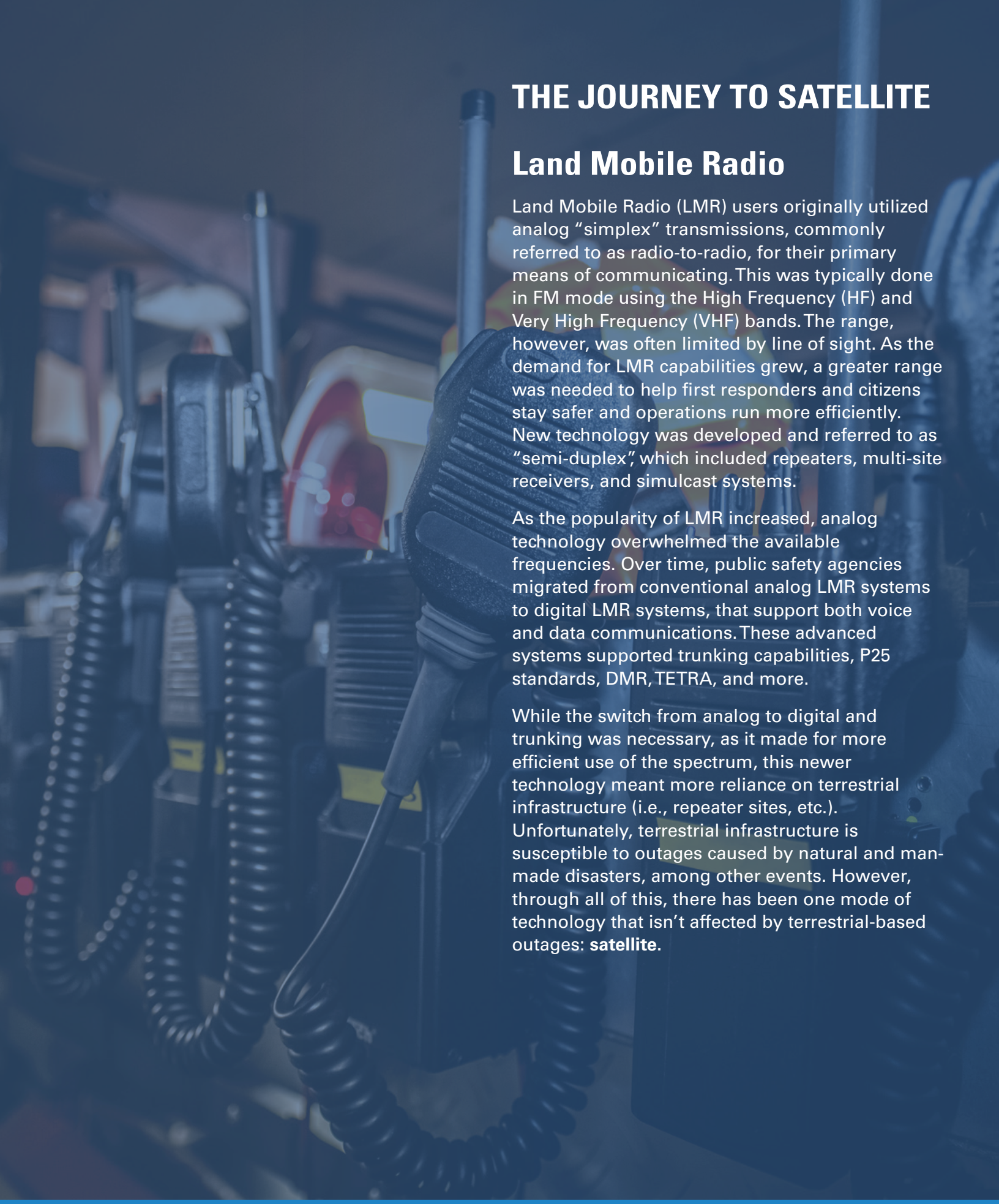


After an emergency, the use of technology is crucial in assisting resources to respond to the scene of an incident. The quicker resources can respond, the sooner the emergency can be mitigated, and the faster normality can be restored. This approach applies to almost any emergency incident such as a car accident blocking traffic flow, a structure fire affecting adjacent buildings, or even a large-scale natural or man-made disaster.

That's where Mission Critical Push-To-Talk (MCPTT) comes in.

Having been around since the 1930s, MCPTT has provided Land Mobile Radio (LMR) users with a migration path to 4G(LTE), 5G, and satellite networks, while retaining their existing capabilities for mission-critical group communication.

To best understand the technologies at play, it's important to look at developments that marked the foundation for the evolution of today's MCPTT capabilities.



THE JOURNEY TO SATELLITE

Land Mobile Radio

Land Mobile Radio (LMR) users originally utilized analog "simplex" transmissions, commonly referred to as radio-to-radio, for their primary means of communicating. This was typically done in FM mode using the High Frequency (HF) and Very High Frequency (VHF) bands. The range, however, was often limited by line of sight. As the demand for LMR capabilities grew, a greater range was needed to help first responders and citizens stay safer and operations run more efficiently. New technology was developed and referred to as "semi-duplex", which included repeaters, multi-site receivers, and simulcast systems.

As the popularity of LMR increased, analog technology overwhelmed the available frequencies. Over time, public safety agencies migrated from conventional analog LMR systems to digital LMR systems, that support both voice and data communications. These advanced systems supported trunking capabilities, P25 standards, DMR, TETRA, and more.

While the switch from analog to digital and trunking was necessary, as it made for more efficient use of the spectrum, this newer technology meant more reliance on terrestrial infrastructure (i.e., repeater sites, etc.). Unfortunately, terrestrial infrastructure is susceptible to outages caused by natural and man-made disasters, among other events. However, through all of this, there has been one mode of technology that isn't affected by terrestrial-based outages: **satellite.**

Satellite Communications

Satellite communication, or "Satcom", plays a vital role in the global telecommunications system by providing a line-of-sight communications path between a ground terminal and a satellite. It's comprised of two main components: (1) the ground segment, consisting of a fixed or mobile user terminal; and (2) the space segment within the satellite itself. The acquired signal is then sent back to earth, where it enters the Public Switched Telephone Network (PSTN).

In the early days of satellite, public safety agencies or organizations would typically use the Inmarsat-A system, and then later Inmarsat-M terminals, to make satellite phone calls and coordinate their responses to an incident. The Inmarsat system is geostationary (GEO), meaning the satellites are positioned around the equator orbiting the earth, and as the earth is moving at the same speed, the satellites appear to remain in the same place. Inmarsat's GEO technology would be used for many years as the go-to for mobile satellite communications and low-speed data connectivity.

In the early 2000's Iridium became the first Low-Earth Orbiting (LEO) constellation, comprised of 66 satellites circling the earth, providing a means of making phone calls to handheld satellite phones.

The Early Days of MCPTT over Satellite

Mission Critical Push-To-Talk (MCPTT) services connect first responders, homeland security, and other public agencies – and over the years, have rapidly evolved to work through the technological challenges of interoperability. The first use of MCPTT over satellite was used by World Space Agencies to communicate with astronauts. In the late 1980s, NASA permitted the American Red Cross, among other agencies and organizations, to use a little-known satellite called ATS-3 for MCPTT, helping deliver enhanced communications capabilities among public safety agencies and personnel in emergency situations.

Until the 1990s, the use of MCPTT over satellite in the United States, by anyone other than a government or quasi-governmental agency, was virtually non-existent.

MSAT PTT: History

In the early 1990s, the former American Mobile Satellite Corporation (AMSC), later becoming Mobile Satellite Ventures (MSV), launched and operated two satellites covering North America. In 2008, MSV changed its name to SkyTerra, going on to replace the two original satellites. In 2010, under new leadership, SkyTerra became part of a new company called LightSquared – which later sold its satellite airtime business to Network Innovations.

Through all of the changes and acquisitions, the technology remained the same – MSAT PTT became the standard in Mission Critical Push-To-Talk (MCPTT) for many local, state, and federal first responders operating in North America. Finally, in 2016, LightSquared announced its new name: **Ligado Networks.**

Between the late 1990s and the present day, the use of satellite PTT by public safety and emergency response agencies has grown exponentially. The MCPTT voice service over satellite on SkyTerra-1 is now known as "MSAT" and utilizes the MSAT-G2 and the latest MSATe user terminals.

Present Day

Today, Network Innovations' proven reliable MSAT PTT service, powered by Ligado Networks, has both a MCPTT capability and the ability to make and receive regular telephone calls through the Public Switched Telephone Network (PSTN). The MCPTT functionality is capable of 1-1 or one-to-many communications via multiple talkgroups.

While some large agencies, like FEMA or the Red Cross, may create their own internal talkgroup(s), there are also SMART Talkgroups (Satellite Mutual-Aid Radio Talkgroup) that have been created and used as a means of interoperability between federal agencies and organizations for many years.

PRESENT-DAY MSAT AND INTEROPERABILITY

Satellite Mutual-Aid Radio Talkgroup (SMART™)

In the past, communications technologies were designed to meet the needs of individual agencies, with limited interoperability. The ability to communicate across agencies was unreliable. This resulted in communication gaps that could lead to loss of life or property, as well as delays in response time.

The need for reliable, interoperable communications was clear in the wake of Hurricane Katrina. However, the Gulf region and other areas prone to hurricanes were not the only places in need of this type of technology. Wildfires, earthquakes, tornados, snowstorms, and other natural or man-made disasters such as 9/11, the Oklahoma City bombing, and hostage situations, all required reliable inter-agency communications to ensure the safety and security of the public.

Achieving interoperable communications nationwide was an increasingly high priority for policymakers and the public safety and emergency response communities. It was this growing concern that led the FBI and the Department of Justice (DOJ) to approach LightSquared with an idea that would initiate the Satellite Mutual Aid Radio Talkgroup (SMART™) program.

About The SMART™ Program

SMART™ is a satellite-based service that connects federal, state, local, and tribal public safety professionals via numerous overlapping national and regional talkgroups. The SMART™ program is designed to tackle the financial and governance challenges that have often impeded the development of interoperable public safety communications. Successfully deployed across all 50 states, it has provided law enforcement agencies with access to their own private radio channels, as well as access to any other channel throughout the country at no cost.

The MSAT satellite network delivers the utmost reliability and interoperability. A satellite link is available even when cell towers and landlines are congested or damaged and is accessible from remote areas that aren't served by terrestrial networks. During Hurricane Katrina, many emergency operations centers had to be evacuated. In these situations, public safety officials need the ability to communicate with each other and other first responders, even when their headquarters aren't operational.

The mobility of MSAT satellite terminals ensures that public safety officials can communicate under any circumstances. In addition, MSAT's dispatch style, Push-To-Talk technology is familiar to first responders and optimal for incident command and control.

With SMART™ talkgroups, you can expand your PTT capabilities and interoperability exponentially – this means if users are already utilizing a local system, they can join and easily coordinate with other teams. Many governments and public safety organizations across the country are current Network Innovations MSAT subscribers. **To reduce financial barriers, Ligado Networks and Network Innovations offer SMART™ talkgroups free of charge to anyone who already uses an MSAT Push-To-Talk (PTT) service with Network Innovations.**

The management of SMART™ is entirely in the hands of the people who know public safety best. Each SMART™ talkgroup is managed and monitored by a different public safety entity – ensuring design, control, and management by officials through multiple public-private partnerships.

There are both Nationwide and Regional SMART™ talkgroups, both are shown below.

Nationwide SMART™ Talkgroups[1]

J-SMART
Public Safety
Federal Bureau of Investigation

F-SMART
Fire Service
City of Seattle Fire Department

NPHST-1 / NPHST-2
Public Health
KY Department for Public Health

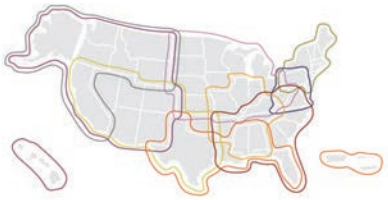
I-SMART
Critical Infrastructure
Seattle Public Utilities

E-SMART
EMS
KY Department for Public Health

L-SMART
Law Enforcement
U.S. Marshals Service

U-SMART
Urban Search & Rescue
Montgomery County (MD) Fire & Rescue Service

Regional SMART™ Talkgroups[1]



NESMART
CT, DE, MA, ME, NH, NY, NJ, PA, RI, & VT
CT State Police

MWSMART
IA, IL, IN, KS, KY, MI, MN, MO, OH, ND, NE, SD, WI, & WV
IN Department of Homeland Security

M-SMART
DC, DE, MD, PA, VA, & WV
Allegany County (MD) Dept. of Public Safety and Homeland Security

SWSMART
AZ, CA, CO, NM, NV, OK, TX, & UT
Contra Costa County Fire Protection District

SESMART
AL, AR, DC, FL, GA, KY, LA, MS, NC, SC, TN, VA, & WV
Fairfax Co. (VA) Comm./Fire Rescue

NWSMART
AK, CA, ID, MT, OR, WA, & WY
Washington State Emergency Management Division

G-SMART
AL, FL, LA, MS, TX, PR, & USVI
Texas Division of Emergency Management

W-SMART
AK, AZ, CA, CO, HI, ID, MT, NM, NV, OR, UT, WA, & WY
CA Emergency Management Agency

CUSEC-1
AL, AR, IL, IN, KY, MS, MO, & TN
Central United States Earthquake Consortium

MSAT PTT to LMR Interoperability

In no other industry is evolution more inevitable than satellite tech. Eventually, organizations wanted the ability to expand the on-the-ground functional use of a MSAT-G2 user terminal, and they did so. Transportable and mobile kits were created to enable users to extend their terrestrial range, and thus radio to satellite PTT was born.

Connecting the MSAT-G2 satellite PTT with Land Mobile Radio (LMR) was a natural progression. Although it would seem easy to connect the two, there are inherent challenges in doing so. One of the biggest hurdles was ensuring a two-way radio transmission could get through in a public safety environment, where PTT traffic is considered mission critical. To address this complex issue, Network Innovations created an innovative satcom talk-tone delay and playback solution to ensure mission critical PTT messages would be received, no matter the status of the MSAT satellite talk path. SATRAD Matrix was born.

MSAT PTT Interoperability Using SATRAD

SATRAD Matrix mSeries and iSeries provide mission-critical Push-To-Talk reliability via an easy-to-use gateway – ensuring a line of satellite to two-way radios and other devices. Built to bridge MSAT or Iridium PTT and LMR, this solution offers immunity from disruptions to traditional radio infrastructure such as earthquakes, power outages, and weather events.

Ensuring full two-way radio service across North America, SATRAD enables organizations to utilize a single satellite-to-LMR solution for communications across the continent. The SATRAD Matrix system is interoperable with most mobile two-way radios and dispatch console systems and can be utilized as a primary or emergency backup solution in the event that terrestrial communications fail.

Interoperability Gateways (Analog)

Similar to Network Innovations' SATRAD Matrix gateways, other solutions were designed and built with interoperability in mind. One is the JPS ACU-1000 Interop gateway – the first device built to bridge different radios together enabling same-band and cross-band interoperability between multiple public safety two-way radios and agencies. Eventually, other manufacturers worked on making their own gateway(s), however, JPS proved itself to be one of the most trustworthy interop gateways available.

Interoperability Gateways (IP)

The arrival of Internet Protocol, or IP as it is commonly referred to, enabled analog or digital two-way radios to connect to newer IP-enabled gateways – allowing for a common platform for multiple different two-way radios to communicate with each other globally, via a local LAN or WAN. This enabled disparate radio systems to be connected to one another in a "virtual talkgroup" over IP. The door to radio interoperability between agencies and organizations was opened.

In 2005, Hurricane Katrina was one of the first large-scale disasters to use Radio-over-IP (RoIP). The American Red Cross used RoIP to dispatch vehicles throughout the gulf coast from Falls Church, Virginia. The system was built with multiple "packages" of Ku-Band VSAT satellite terminals mated to VHF Low-Band donor base radios using a Telex-Vega IP-223 IP-enabled gateway. This solution proved that RoIP could be used reliably in a large-scale disaster, as long as you had a VSAT satellite or other proven reliable internet connection available.

There are many different IP-enabled interoperability gateways available today – each one with different features and functionalities.

ENHANCED GROUP COMMUNICATIONS WITH IRIDIUM PUSH-TO-TALK

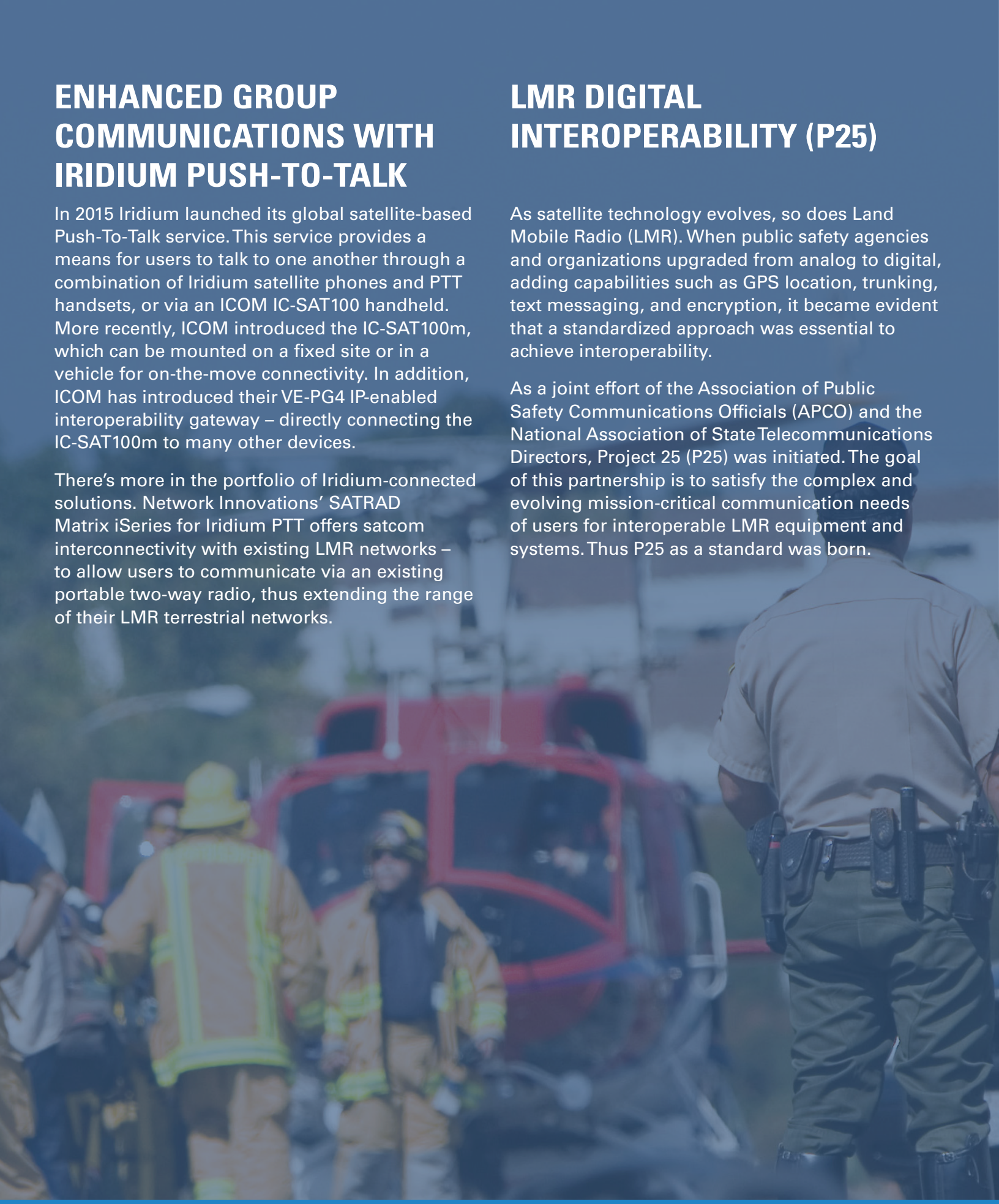
In 2015 Iridium launched its global satellite-based Push-To-Talk service. This service provides a means for users to talk to one another through a combination of Iridium satellite phones and PTT handsets, or via an ICOM IC-SAT100 handheld. More recently, ICOM introduced the IC-SAT100m, which can be mounted on a fixed site or in a vehicle for on-the-move connectivity. In addition, ICOM has introduced their VE-PG4 IP-enabled interoperability gateway – directly connecting the IC-SAT100m to many other devices.

There's more in the portfolio of Iridium-connected solutions. Network Innovations' SATRAD Matrix iSeries for Iridium PTT offers satcom interconnectivity with existing LMR networks – to allow users to communicate via an existing portable two-way radio, thus extending the range of their LMR terrestrial networks.

LMR DIGITAL INTEROPERABILITY (P25)

As satellite technology evolves, so does Land Mobile Radio (LMR). When public safety agencies and organizations upgraded from analog to digital, adding capabilities such as GPS location, trunking, text messaging, and encryption, it became evident that a standardized approach was essential to achieve interoperability.

As a joint effort of the Association of Public Safety Communications Officials (APCO) and the National Association of State Telecommunications Directors, Project 25 (P25) was initiated. The goal of this partnership is to satisfy the complex and evolving mission-critical communication needs of users for interoperable LMR equipment and systems. Thus P25 as a standard was born.



ENCRYPTION

Encryption is the process of encoding information in a way that only authorized parties can access it – enabling secure and effective radio communications in an increasingly digital environment. For traditional transmit and receive radio, or two-way radio, encryption modifies a voice signal using a coded algorithm. This algorithm is controlled or accessed by an encryption key, which is used by the transmit and receive radios to enable the voice signal to be coded and decoded for both radios. Therefore, all radios communicating must have matching encryption keys to receive transmissions.

For many agencies and organizations, secure communication is a necessity. For example, a SWAT team running a covert operation would not want a third party to intercept or listen in on their communications.

While encryption protects critical information, using it requires enhanced interoperability during joint emergency response efforts. If one responder agency uses an encryption key that hasn't been shared with the other parties involved, then group communication would be impossible, hindering interoperability.

This is a challenge beyond the scope of this paper that needs addressing. However, the takeaway is that MCPTT between multiple agencies and organizations is critical, and planning for any incident should be done in advance to ensure seamless interoperability.

PRIORITY ACCESS SERVICES (FIRSTNET)

In emergencies and disasters, commercial networks can quickly become congested, meaning communications aren't available to first responders when they need it most. To combat this issue, the U.S. government created a program allowing commercial wireless and landline providers to offer Priority Access Services to public safety personnel. Offered at federal, state, and local levels, this program enabled responders to communicate with minimal interruption – cutting through network congestion. The three solutions for priority access included: (1) Government Emergency Telecommunications Service (GETS); (2) Telecommunications Service Priority (TSP); and (3) Wireless Priority Services (WPS). These services are still available today through CISA.GOV.

Since MCPTT is primarily wireless, this program would be supported by AT&T, T-Mobile/Sprint, and Verizon, among other regional wireless carriers. Following the attacks on 9/11, the public safety community worked diligently to urge congress to establish a single nationwide network, allowing all public safety agencies to communicate. As a result, the FirstNet Authority was established and deployed through a first-of-its-kind public-private partnership between the federal government and AT&T. FirstNet offers the public safety sector a terrestrial cellular broadband communications network – built to their operational and technical needs to help them save lives and protect our communities.

First Responder Network Authority, or FirstNet Authority, is the federal entity charged with overseeing the building, deployment, and operation of the FirstNet network. Established as an independent authority within the U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), the agency's role is to establish a network that equips public safety with broadband communications services, now and into the future, and ensure AT&T delivers on the terms of its contract.

As part of the agreement, AT&T can utilize the FirstNet spectrum when it's not in use by public safety for other commercial purposes. The company will prioritize first responders, however, over any commercial users. They do this by using Band 14 and certifying 4G(LTE) and 5G devices as "FirstNet Ready" to be used on this network specifically for public safety and other supporting agencies and organizations.

While FirstNet is an important step in ensuring MCPTT, it's important to keep in mind best practices of resiliency includes employing terrestrial wireless and satellite carrier diversity in your edge networks. Recent disasters have shown even the most experienced user/responder that multiple paths of connectivity are always better than one.

2G,3G,4G(LTE), AND 5G

While LMR is currently the go-to technology for public safety MCPTT, it is costly to build these systems and the complexities can be cost-prohibitive for some state and local entities to implement.

In the early 2000s, Nextel introduced an Integrated Digital Enhanced Network (IDEN) based PTT service called Direct-Connect. This became popular with the public safety community and enabled nationwide MCPTT features with the help of Motorola. Nextel was a success. But as technology evolved, Nextel did too, and the IDEN network was shut down after the merger with Sprint. Verizon, Sprint, and Cingular created PTT applications, however, at the time they didn't catch on with public safety as Nextel did. Interoperability between agencies and organizations really can't be achieved without a nationwide plan in place – this is why FirstNet was created.

3G, 4G(LTE), 5G, (FIRSTNET) AND APPLICATIONS

As providers addressed the need to offer PTT functionality over cellular, android and iOS PTT applications were created. These technologies didn't take off with public safety users until FirstNet was created, leading to a resurgence of FirstNet Ready and FirstNet Certified Applications introduced into the public safety marketplace. Some of the first applications included Motorola Wave, Kodiak, ePTT, FirstNet PTT, ESChat, and JPS VIA. There are currently many applications available in the FirstNet Applications catalog that can be used by Public Safety entities for PTT, as well as voice, data, tracking, and video applications.

These applications start to blur the lines of technology between LMR and traditional 3G,4G(LTE), and 5G systems. However, it's important to note that all of these applications are referred to as Over-The-Top (OTT) – being applications that simply traverse the 4G(LTE) and 5G (FirstNet) networks, not delivering MCPTT as public safety officials would expect. Work is underway to build PTT solutions at 3GPP standard for MCPTT, which meet or exceed the performance of public safety standards when a user device is connected to a 4G(LTE) and 5G network, similar to P25 and TETRA.

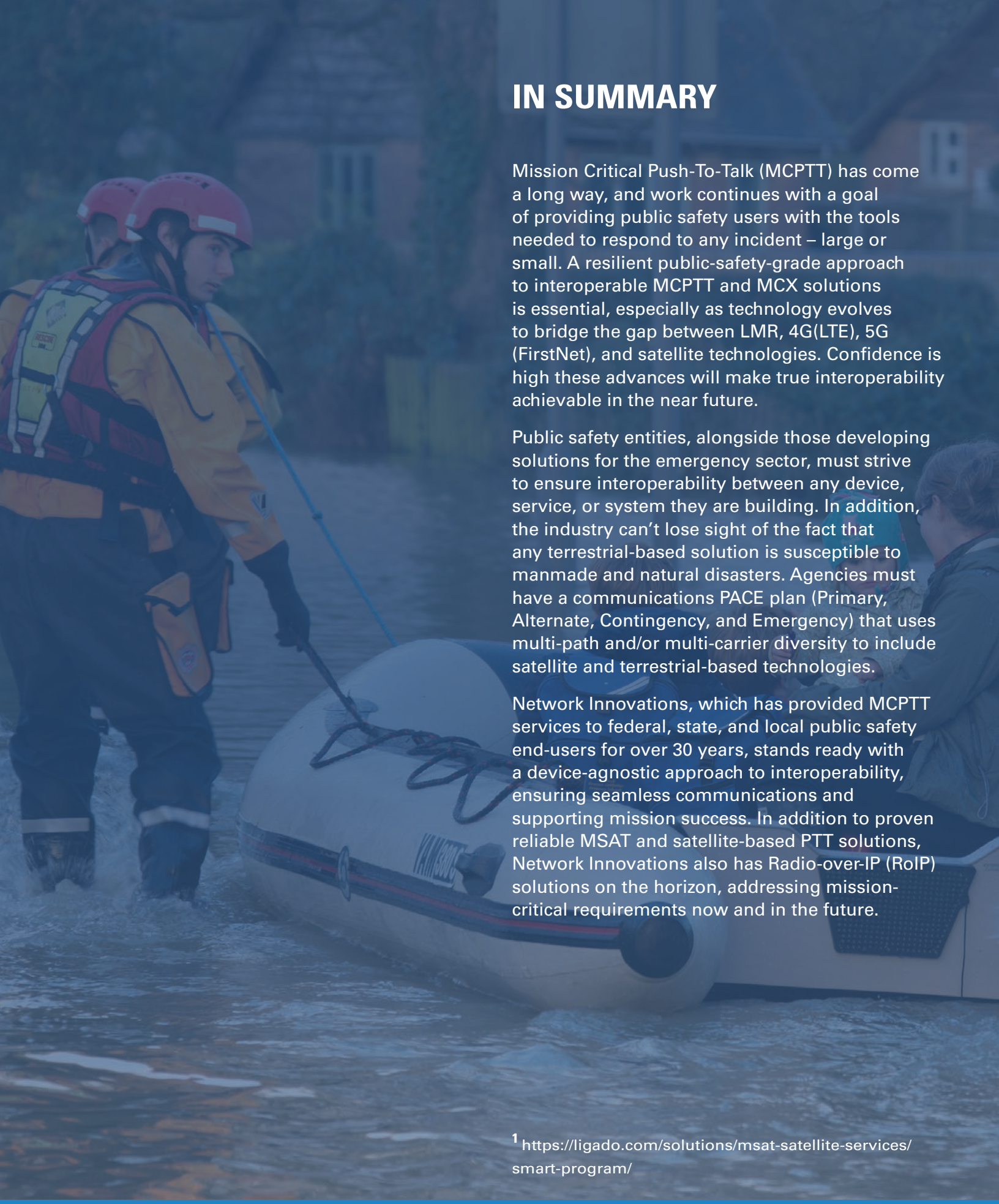
In order to maintain a standard for interoperability, especially as it pertains to MCPTT – 3GPP was born.

3GPP AND MCX (A STANDARD FOR INTEROPERABILITY)

The 3rd Generation Partnership Project (3GPP) is a global standard body, working to build standards for 3G, 4G (LTE), and 5G. 3GPP has defined the Mission Critical (MCX) services standard which will enable mission critical services like Push-To-Talk (PTT), data, video, and other services to run on 4G(LTE) and 5G systems.

At the 2022 APCO Conference, FirstNet revealed that "FirstNet PTT", developed by Samsung, is designed to meet the 3GPP standard for MCX. Robert Fowler, AT&T's product management specialist for FirstNet LTE mission-critical services stated: **"The solution is a high-prioritized solution on the network,"** Fowler said during the APCO presentation. **"One of the key differences between FirstNet Push-To-Talk and any application you might download from Google Play or iTunes is that this is really a core network service – not an application. It is part of the LTE network, fully integrated with an enhanced packet core. So, it's not an external entity that's connected to the FirstNet network. It's an integral part of the FirstNet solution. Therefore, we can prioritize the service more than you can any standard, over-the-top application. It delivers on the 3GPP promise of a low-latency, high-performing audio-quality service, and you'll note that, if you test the service out yourself."**

This is evident of progression within MCPTT, there is still a need to connect MCPTT to LMR using RoIP (Radio-over-IP). Release 17 of the 3GPP standard introduces interoperability using the Interworking Function (IWF). As Fowler indicated: **"IWF is part of the MCX infrastructure, so each of the solutions has a different approach. Down the FirstNet PTT approach, we're using Samsung and Etherstack core software. So, ISSI guys—with a premier network-infrastructure player—are building IWF".**



IN SUMMARY

Mission Critical Push-To-Talk (MCPTT) has come a long way, and work continues with a goal of providing public safety users with the tools needed to respond to any incident – large or small. A resilient public-safety-grade approach to interoperable MCPTT and MCX solutions is essential, especially as technology evolves to bridge the gap between LMR, 4G(LTE), 5G (FirstNet), and satellite technologies. Confidence is high these advances will make true interoperability achievable in the near future.

Public safety entities, alongside those developing solutions for the emergency sector, must strive to ensure interoperability between any device, service, or system they are building. In addition, the industry can't lose sight of the fact that any terrestrial-based solution is susceptible to manmade and natural disasters. Agencies must have a communications PACE plan (Primary, Alternate, Contingency, and Emergency) that uses multi-path and/or multi-carrier diversity to include satellite and terrestrial-based technologies.

Network Innovations, which has provided MCPTT services to federal, state, and local public safety end-users for over 30 years, stands ready with a device-agnostic approach to interoperability, ensuring seamless communications and supporting mission success. In addition to proven reliable MSAT and satellite-based PTT solutions, Network Innovations also has Radio-over-IP (RoIP) solutions on the horizon, addressing mission-critical requirements now and in the future.

[1] https://ligado.com/solutions/msat-satellite-services/smart-program/

ABOUT THE AUTHOR
Steve Hailey, PTT Product Director

Steve Hailey has 30 years of experience in public safety and emergency communications and has seen firsthand the effects of manmade and natural disasters on mission critical infrastructure. His role at Network Innovations is to help design, build, and deploy mission critical voice and data products and services for the first-responder community in North America and around the world.

ABOUT NETWORK INNOVATIONS
Your Advanced Connectivity Provider

Since 1989, Network Innovations has grown to be a global leader in connecting people, places, and things with always available solutions. Our dedicated specialists have the depth of training and experience to design, build, and execute the most successful technology solutions for the unique needs of government and defense, public safety, oil and gas, media, mining, utilities, maritime and recreation and leisure. We are a trusted partner empowering our clients to *Succeed. Anywhere.*

NETWORK INNOVATIONS