Lessons Learned from Global Attacks:
How FirstNet Can Better Prepare the U.S. for Crisis Response

Introduction

Terror attacks and mass shootings have become far too common in our world today, and public safety officials across the United States are forced to plan and prepare for worst-case scenarios in their own communities. As terrorist tactics continue to evolve, so too must the law enforcement response.

Patterns can be found in after-action analysis of incidents around the globe and here at home. Recurring problems hindering law enforcement include communication breakdowns among responding agencies, overcrowded cellular networks, and a lack of real-time information sharing at the scene of the attacks.

Our nation has an opportunity to incorporate lessons learned from crises worldwide into the ongoing development and deployment of the FirstNet (First Responder Network Authority) nationwide public safety broadband network (NPSBN). Established to modernize communications for first responders and provide a dedicated high-speed broadband network exclusively for public safety, FirstNet can make significant strides toward better preparing and equipping U.S. first responders for large-scale emergency scenarios.

Secure, Interoperable Communications

One of the biggest hurdles to overcome when faced with a large-scale incident is a lack of communication systems interoperability. Public safety officials – police, fire, EMS, SWAT, FBI, and more – responding to an incident cannot effectively communicate with each other (interoperate) in real time. Often they have disparate radios and systems, operate on different frequencies, or simply have no means to connect with one another seamlessly and securely.

Sadly, this crucial functional deficit was identified long ago in the aftermath of the September 11, 2001 terrorist attacks. A report by the federal 9-11 Commission found that "rescuers were forced to make rapid-fire, life-and-death decisions based on poor communications, contributing to the World Trade Center death toll. Communications breakdowns also prevented announcements to evacuate from reaching civilians in the building. Those were only a few of the widespread communication problems found by the investigation. Firefighters used different radio channels. Public address systems and intercoms failed" (*CBS News, May 18, 2014*).

Fast-forward 13 years to Aurora, Colorado, where interoperability problems were found to be a central problem in the response to the movie theater shooting. An after-action report concluded that "a breakdown in police and fire communication resulted in a chaotic response to treating victims of the Aurora theater shooting. Police officers didn't know how to communicate directly with fire officials as they confronted hordes of blood-soaked victims streaming toward them. Members of the theater audience had better cellphone communications with each other than did police and fire personnel," the report notes (*Denver Post, October 8, 2014*).

> **In Aurora, Colorado,**
> *"Members of the theater audience had better cellphone communications with each other than did police and fire personnel."*
> Denver Post, October 8, 2014

How FirstNet Can Get It Right

A fundamental goal of FirstNet is to enable communication and collaboration capability between all first responder agencies. FirstNet defines interoperability as "*the ability of all authorized local, state and federal public safety entities and users to operate on the NPSBN (National Public Safety Broadband Network) and commercial partner networks, to access rapid, reliable and secure communication services, in order to communicate and share information via voice and data.*"

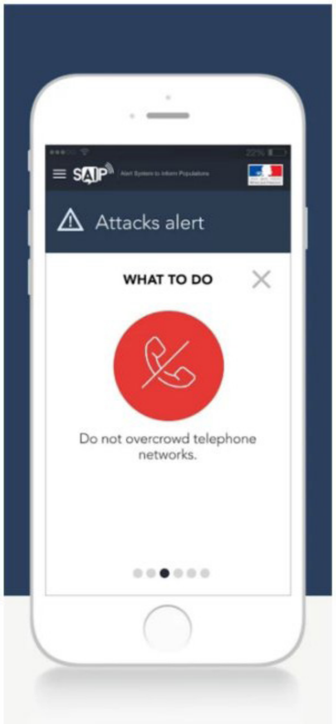
To achieve this goal, the collaboration capability must be core to the FirstNet architecture and include network, device and agency interoperability. It's worth noting, too, that for many large-scale incidents, the need to collaborate with non-FirstNet agencies such as schools, utilities, mass transit, and others, including public safety agencies that have not yet migrated to FirstNet, will improve outcomes. The opportunity to achieve truly ubiquitous multi-agency collaboration will only be possible if FirstNet users and non-FirstNet participants can securely connect and share information in an emergency.

Dedicated High-Speed Broadband Network

Another fundamental problem faced by first responders during recent terror attacks was overcrowded cellular networks, which impeded communications and situational awareness for responding authorities. And it's not only unplanned crises that can overload the cellular infrastructure – so too can mass gatherings like a major sporting event or concert. When tens of thousands of cell phone users compete for the limited resources of commercial cellular networks, the result is poor data transmission, dropped and incomplete calls.

In the aftermath of the terror attacks in Brussels in March 2016, various media sources reported that Brussels police were forced to use WhatsApp Messenger to communicate with one another in the wake of the attacks, and that widespread communication problems hampered emergency services. ASTRID (Belgium's public-safety network provider) experienced "network saturation," leaving law enforcement unable to connect and collaborate in the chaos. ASTRID's own analysis after the attacks concluded that some of its base stations in Brussels reached their maximum capacity (saturation), preventing some communications from proceeding trouble free (*Mission Critical Communications, May 19, 2016*).

In neighboring France, authorities sought to alleviate network congestion during emergencies and created an instant alert app that warns the public, "**Do not overcrowd telephone networks**" during an attack. Sadly, the Bastille Day tragedy in Nice was the first time the app was put to the test, and a "technical glitch" caused the alert to be issued a full three hours after the incident.



Do not overcrowd telephone networks.

The Foresight of FirstNet

A primary purpose of FirstNet is to deploy a dedicated high-speed wireless broadband network for public safety, which will eliminate problems caused by congested commercial networks. With Band 14 spectrum allocated exclusively for FirstNet, substantial bandwidth will be available for public safety applications. For those times when more bandwidth is needed – such as for video sharing or rural, remote locations – innovative solutions are being tested to implement deployable networks utilizing Systems on Wheels (SOWs) and Cells on Wheels (COWs). This approach provides for enhanced local resiliency and reduced latency of the media. Deployed SOWs and COWs are highly resilient and able to access the network through satellite and/or microwave, even when cell tower infrastructure is compromised. This addresses the needs of rural areas, as well as natural disaster situations or terrorist infrastructure attacks.

JerseyNet – New Jersey's FirstNet implementation – is an "Early Builder" project and the first in the nation to utilize deployable networks. JerseyNet proved successful in 2015 for two high-profile beach concerts in Atlantic City, which attracted nearly 100,000 fans. Police officials reported "Zero Loss of Data" during the busy events. "This was the first time during a large, densely populated event that we were able to maintain a constant real-time video stream, and this vastly improved the situational awareness for everyone involved with securing these events," said Lieutenant James A. Sarkos Atlantic City Police Department BTOP Project Manager. In addition, interoperability across state lines provided secure communications over JerseyNet during the 2015 Papal visit in Philadelphia.

Real-Time Video Sharing

While many cities and facilities are investing heavily in security and surveillance cameras, they are traditionally used to record footage for play-back after an incident has occurred. This is also the case with law enforcement body cameras, which are becoming more prevalent in police departments nationwide. It would significantly improve situational awareness for first responders if video footage could be viewed – and shared – by first responders at the scene as events are unfolding, as well as between the incident scene and command center.

Following the attack on the Charlie Hebdo headquarters in Paris, it was found that "the most important piece of video imagery to emerge from the siege, at least in the hours after the event occurred, was taken on a phone belonging to a person near the scene" (*Defense One, January 7, 2015*).

According to Lt. Michael Stark, one of law enforcement's challenges regarding real-time streaming video is "interoperability between systems. Video systems and the software used to view and operate them are not always compatible with other systems. A school district, stadium, mall or other business may have a state-of-the-art video surveillance system in place; however, due to software incompatibility, they may not be able to share that system with another agency" (*Law and Order, September 2011*).

FirstNet Multimedia Collaboration

One of the most anticipated capabilities of FirstNet is the ability to video conference and share video feeds within and between agencies. A dedicated high-speed network, combined with advanced multimedia sharing technologies, will enable unprecedented inter-agency communication and situational awareness.

Atlantic City public safety personnel using JerseyNet benefited from this capability last summer. "Video assets are paramount with events like beach concerts where crowd density is elevated. Real time, reliable video acts as a force multiplier and gives the added ability to deploy reaction teams to precise locations to deal with emergencies or prevent an incident from escalating," said Deputy Chief William Mazur Incident Commander for Atlantic City Beach Concerts.

While many agencies are equipped with traditional LMR push-to-talk (PTT) capability, mobile devices using multimedia interoperability apps deliver the added benefits of "push-to-see" real-time video sharing. In this way, FirstNet combines the convenience of a narrowband PTT radio with the extraordinary power of a smartphone – all connected to a secure, nationwide multimedia broadband network.

Our Society of Silos

A silo describes any system that is unable to operate with any other system. It is closed off from other systems, creating an environment of individual and disparate systems within an organization. Communications silos abound in our communities. Public agencies and private entities want to protect their own resources and assets, and maintain full control over who has access to that information.

Although silos are necessary constructs for maintaining agency sovereignty, privacy and control, they pose a significant disadvantage when multiple agencies need to work together during events or emergency incidents. Mutual response requires agencies to share information and communications to be effective in working together. It is in these situations where silos present an obstacle to the required collaboration.

In a 2012 speech, Gil Kerlikowske, Director of the Office of National Drug Control Policy, discussed the need to break down silos between law enforcement and public health when it comes to drug policy. "Silos, like specialties, can be a good thing. But when the walls between these different silos become so high that the people inside cannot communicate across them, the effectiveness of the organization suffers."

Silos are prevalent in government, law enforcement, and intelligence communities worldwide. Following terror attacks in France, it was reported that, “The French law enforcement bureaucracy is in a permanent state of reform, but the services still often work in their own silos. For example, there is a cooperation gap between the gendarmerie, which polices rural France, and domestic intelligence” (*Chicago Tribune, July 15, 2016*).

Bridging Silos with FirstNet

First and foremost, FirstNet should recognize that silos are not going away, so it’s imperative that we find an effective way to work with them. To do this, FirstNet must ensure security for all parties through access control and encryption, and maintain the sovereignty of owning agencies. FirstNet should also enable ad hoc sharing of information and resources under the control of agency personnel on the scene.

One way to achieve this is to selectively and securely bridge existing silos together. In this way, “selective” information can flow between silos when and as needed. This can be accomplished in the absence of a central server or switch, overcoming concern about undesired third-party control, and individual parties maintain their sovereignty. By bridging silos, first responders will have access to crucial – potentially life-saving – information that will significantly improve situational awareness during emergencies.

Mutualink and FirstNet

The Mutualink solution was designed from the ground up as a highly-reliable distributed system to fully optimize the opportunity for public safety and related agencies to collaborate in real time using a variety of media. Mutualink enables inter-agency collaboration with voice, video, text, and data.

> *“Public safety agencies don’t have to wait for FirstNet to be fully-operational to reap the benefits of inter-agency interoperability,” said Colin McWay, President of Mutualink.*

The system was built on the foundational principle of sovereignty – that every participating agency should maintain complete control of the assets they are sharing with others. There is no centralized server or switch to which systems must be connected in order to interoperate, and only an IP network is required. This key differentiator, along with full multimedia capability and distributed resiliency, make the Mutualink system a perfect complement to FirstNet.

Mutualink’s technology leverages the capabilities of the FirstNet public safety network by bridging all forms of communications assets to provide a dynamic and rich media collaboration environment. Mutualink’s effectiveness also extends beyond FirstNet by connecting not just first responders, but also Critical Infrastructure and Key Resources (CIKR) such as hospitals, schools, utilities, shopping malls, corporate security and more.

Mutualink’s Experience in FirstNet Projects

Mutualink has participated in several FirstNet Early Builder projects and Band 14 demonstrations, providing cross-agency collaboration by connecting disparate video management systems, radio systems and mobile devices – including LMR to LTE. Examples include:

- In **2013**, Mutualink was used by multiple public safety and enterprise entities connected to the Band 14 LTE network deployed in Las Vegas, Nevada.
- Since **2014**, Mutualink has been used on the Band 14 LTE system in Harris County, Texas – the nation’s first operationally deployed public safety LTE network.
- In **February 2015**, Mutualink participated in a field-demo in Adams County, Colorado – a FirstNet Early Builder project.
- In **September 2015**, Mutualink played a central role in the “FirstNet in Motion” Urban Shield exercises in Alameda County, California.

- In **October 2015**, a Wearable Smart Gateway device – developed by Mutualink and Intel – was used in conjunction with the FirstNet Band 14 during the International Balloon Fiesta in New Mexico.
- Mutualink was selected for inclusion in JerseyNet, which has been utilized for numerous events including Pope Francis' visit to the U.S. in **2015** and high-profile beach concerts in Atlantic City.
- In **February 2016**, Mutualink's technology was used during Super Bowl 50 in California to provide interoperable communications over the Band 14 network.
- In **July 2016**, Mutualink was used in conjunction with a Band 14 LTE network to cover the "expressive zones" — also known as protest areas — for the Republican National Convention in Cleveland, Ohio.

Conclusion

When terror strikes, an effective emergency response requires massive cooperation and information sharing among law enforcement agencies and federal, state and local agencies to eliminate the threat and minimize causalities. First responders must be able to communicate in real time with relevant parties for ongoing assessment and rapid decision-making during unfolding situations.

As FirstNet continues to move closer to nationwide implementation, let's not squander the opportunity to learn from the tragedies that have preceded it. The safety and security of our nation is at stake, and we have the power – and the tools and technologies – to make a difference.

Mutualink, Inc.

Connecticut Headquarters
1269 South Broad Street
2nd Floor
Wallingford, CT 06492

Phone: (866) 957-5465

Research & Development Facilities
3 Lan Drive
2nd Floor
Westford, MA 01886

313 So. Jupiter Road
Suite 110
Allen, TX 75002

E-Mail: info@mutualink.net

Development Facility
Western Industrial Park
Rochelaise # 26 Bo. Guanajibo
Mayagüez, PR 00682

Web: www.mutualink.net