NPSTC
National Public Safety Telecommunications Council

Public Safety Broadband Network Innovation Alliance

2022-2032 Assessment of Future Spectrum and Technology

June 24, 2024

American Association of State Highway and Transportation Officials | American Radio Relay League | Association of Fish and Wildlife Agencies | Association of Public Safety Communications Officials | Forestry Conservation Communications Association | International Association of Chiefs of Police | International Association of Fire Chiefs | International Municipal Signal Association | National Association of State Emergency Medical Services Officials | National Association of State Foresters | National Association of State Technology Directors | National Council of Statewide Interoperability Coordinators | National Emergency Number Association | National Sheriffs' Association

TABLE OF CONTENTS

BACKGROUND

The National Public Safety Telecommunications Council (NPSTC) is a United States based federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications.

The Public Safety Broadband Network (PSBN) Innovation Alliance (PIA) is a Not-for-Profit Alliance of Public Safety entities in Canada focused on advocating for a PSBN policy that will provide access to broadband voice and data services wherever First Responders operate.

On June 5, 2012, NPSTC published the Assessment of Future Spectrum and Technology (AFST) identifying public safety communications requirements for the 10-year period from 2012 to 2022 and to assess the impact on technology and radio spectrum. Since 2012, Public Safety's increased dependence on data through a variety of networks has exposed the need to create another assessment.

The Assessment of Future Spectrum and Technology (AFST) 2022-2032 is an updated report to address the Operation, Spectrum, and Technology needs for the next 10 years. NPSTC has also secured participation and support from Canada's Public Safety Broadband Network Innovation Alliance (PIA), a NPSTC Associate Member, as their telecommunications needs are essentially similar.

NPSTC and PIA recognize that since 2012, the utilization of broadband data applications among public safety entities has grown tremendously. And as the AFST 2022 – 2032 Survey shows, the utilization of data applications is expected to grow further. The survey also underscores that voice communications will remain an important tool as data applications grow.

SURVEY

In the Spring of 2023, NPSTC and PIA jointly conducted a survey of public safety entities in the United States and Canada. The questionnaire was developed by public safety communications practitioners with expertise in areas such as Operations, Technologies, and Spectrum.

The survey queried the size of the entity, the type of government that the entity serves, and the functions the entity currently uses. The survey also asked the entities to assess the future communication needs for Voice, Data, and Video. The survey had 69 questions divided among Dispatch, Law, Fire, Emergency Medical Service (EMS), Search and Rescue, and Other (such as Emergency Management Agency, EMA).

PARTICIPATION

Ninety-six (96) entities responded to the questionnaire and provided input for their future needs. Although participation in the survey failed to produce the quantity of responses desired by NPSTC and PIA, there was enough of a cross-section of the responder community to justify publishing this report.

It is possible that the lack of participation can be attributed to one or more of the following factors:

- Successful Public Safety communications spectrum advocacy in the past decade has resulted in reducing previously identified communications challenges.
- The creation of the FirstNet Authority and the increased reliance on State and Regional Interoperable radio networks has relieved local communications personnel of some of the decision-making.
- Communications expertise in Public Safety agencies is in a transition period from primarily radio frequency (RF) centric to a more network-based architecture (IT) centric knowledge.
- With the widespread adoption of statewide communications systems, the number of personnel maintaining public safety communications systems is reduced.

AGENCY/ORGANIZATION

Most responses came from agencies identifying as a mix of urban, suburban, and rural communities. There was an equal balance of local entities specifying urban, or suburban, or rural only. There was lesser participation by State/Provincial entities. The remainder identified as Federal or Tribal.

46% of the entities were from smaller organizations with fewer than 100 employees. Nearly one-fourth of the respondents were from organizations with greater than 1000 employees.

EMS

21 respondents out of 96 identified themselves as EMS, and respondents were asked to rate the importance of interoperability for current or future applications.

Nearly half rated the following as Highly Beneficial:

- Authorization to reroute patients
- Current and forecasted weather conditions
- Hospital status
- On-scene patient medical history (incl. allergies/medications)
- Situational awareness (resource and personnel tracking and status)

Nearly one-third of the respondents rated the following as Highly Beneficial:

- Bed availability/patient at the receiving facility
- Helicopter availability/critical field resources
- Records Management Systems (billing, restocking)

EMS added the desire for secure wireless transmission of patient telemetry. Lastly, 61% of EMS respondents currently use sensors in their operations and the survey shows an additional 20% intend to do so by 2032. 19% indicated no plan to use sensors by 2032.

LAW ENFORCEMENT

19 respondents of 96 identified themselves as Law Enforcement agencies. Respondents were asked how beneficial technologies would be to assist with on-scene operations.

100% of the respondents rated the following as Beneficial to Highly Beneficial:

- Current and forecasted weather conditions
- Records creation automation (voice-to-text, Google Maps, scene photo insertion)
- Situational awareness (resource and personnel tracking and status)
- Thermal imaging (search)

95% of the respondents rated the following as Beneficial to Highly Beneficial:

- Automatic database queries
- Determining the number of people in a vehicle during a traffic stop
- Evacuation information (perimeter, egress, facilities, safe refuges)

90% of the respondents rated the following as Beneficial to Highly Beneficial:

- Substance identification (sniffer)

- Uncrewed aircraft system (UAS)
- Video stream on demand
- Crime Predictive Software

About 79% of Law Enforcement rated the following as Beneficial to Highly Beneficial:

- Control of signal lights when responding to an incident
- Early detection (e.g. gunshots...)

Law Enforcement also indicated a need for technology to assist in mental health issues.

Respondents were asked if their respective agency uses or plans to utilize sensors for capabilities such as body cams, dash cams, or holster sensors. 63% currently use these types of sensors and 31% more plan to use them by 2032. 5% indicated they had no plan to utilize sensors by 2032.

FIRE

28 of 96 respondents identified themselves as Fire agencies. Respondents were asked how important it is to have real-time information on several capabilities.

100% of the respondents rated the following as Beneficial to Highly Beneficial:

- Current and forecasted weather conditions
- Situational awareness (fire perimeter, building footprints/layouts, other mapping tools)
- Situational awareness (resource and personnel tracking and status)
- Thermal imaging

97% of the respondents rated the following as Beneficial to Highly Beneficial:

- Hazardous material monitoring (plume, run-off, other environmental factors)

93% of the respondents rated the following as Beneficial to Highly Beneficial:

- Early detection of fire incidents
- UAS
- Evacuation information (perimeter, egress, facilities, safe refuges)

Additional capabilities were identified such as the need for firefighter location services, real-time video camera access, firefighter biometrics, and remote database access.

When asked if their agency utilizes sensors such as Self-Contained Breathing Apparatus (SCBA) or vital sign sensors, 30% currently utilize such sensors and 40% more plan to utilize them by 2032. 30% indicated they had no plans to utilize sensors by 2032.

SEARCH AND RESCUE

11 of 96 respondents identified themselves as Search and Rescue. Respondents were asked how important it is to have real-time information on certain capabilities.

100% of the respondents rated the following as Beneficial to Highly Beneficial:

- Ability to locate victims behind structural components (concrete buildings)
- Access to aerial imagery (thermal, video)
- Current and forecasted weather conditions
- Search pattern status
- Situational awareness (resource and personnel tracking and status)

When asked if their agency uses or plans to use data from sensors, 64% currently utilize data while 9% more plan to by 2032. 27% of respondents do not plan to utilize sensors in their operations by 2032. Underwater drones were an additional desired capability.

COMMUNICATIONS/DISPATCH

41 of 96 respondents identified themselves as Communications or Dispatch. Respondents were asked how important it is to have the ability to perform certain functions.

100% of the respondents rated the following as Beneficial to Highly Beneficial:

- CAD-to-CAD capabilities

Over 90% of the respondents rated the following as Beneficial to Highly Beneficial:

- Community situational awareness (social media)
- Current and forecasted weather conditions
- Evacuation information (perimeter, egress, facilities, safe refuges)
- Situational awareness (resource and personnel tracking and status)

Over 80% of the respondents rated the following as Beneficial to Highly Beneficial:

- Real-time camera view of locations (caller, responder)
- Remote dispatching

70% or less of the respondents rated the following as Beneficial to Highly Beneficial:

- Artificial Intelligence (incoming call priority, linking events, language translation)
- UAS dispatching

When asked if their Communications/Dispatch agency uses or plans to use data from sensors, 40% (16 respondents) indicated that they currently use data from sensors and 15% (6 respondents) more plan to do so by 2032. Surprisingly, 45% (18 respondents) indicate that they do not plan to use data from sensors.

Though not all 41 Communications/Dispatch agencies answered the next line of questions, 22 agencies indicated they currently use NG9-1-1 with 14 more planning use by 2032, leaving 5 unanswered. 31 agencies receive SMS messages and 7 plan to by 2032, leaving 3 unanswered. 24 currently send SMS messages while 11 plan to by 2032, leaving 8 unanswered. 10 agencies currently can initiate Integrated Public Alert and Warning System (IPAWS) and 20 agencies plan to by 2032, leaving 11 unanswered.

SURVEY RESULTS

A summary of the results of the survey is provided below.

COMMUNICATION SYSTEMS

Survey respondents were asked to describe which technologies/bands they currently use and plan to use by 2032. Unsurprisingly, the use is concentrated in the VHF, UHF, and 700/800 MHz public safety bands, with additional use of commercial broadband voice and data.

SPECTRUM

Over the years, Public Safety communications demands outgrew the spectrum available. As new technologies were developed, additional bands were allocated, and were put into operational use. Accordingly, Public Safety utilizes a variety of bands and technologies/applications. Question #7 of the survey (under Communications Systems) asked respondents to indicate the <u>uses</u> of each band/technology and multiple options were an allowed response. In general, the results show that Public Safety currently utilizes VHF Low band, VHF High band, UHF (including T-Band in some areas), and 700/800 MHz dedicated spectrum primarily for voice operations, with commercial bands primarily used for broadband data. The results also indicate public safety use of satellite, aviation, backhaul, cellular voice, and cellular PTT. The survey results for Question #7 include a wide range of information. Overall, it shows that Public Safety needs a range of communications options available for operations.

UTILIZATION

Question #9 asked respondents to forecast their spectrum utilization in 2032. While some of the individual percentages vary somewhat from those in current use, the results overall show that both voice and broadband data will still be important for Public Safety. The overall modest number of survey respondents creates some difficulty in making more granular conclusions.

When asked if their respective operations needs will be met in 2032, 82% answered **YES**. Collectively, those who answered **NO** explained that funding, coverage, and throughput would keep them from meeting those needs.

When asked if the number of users or channels will increase by 2032, most responders anticipate an increase in both. Fewer responders predicted no change and virtually none indicated a decrease in either users or channels. (Q.15)

SYSTEM CAPACITY

Respondents were asked to rate the Coverage and Capacity of their current **VOICE** system and to forecast Coverage and Capacity of their **VOICE** systems in 2032.

Current CAPACITY for **VOICE** was rated as mostly meeting the respondent's needs (87%). Current COVERAGE was a problem as 37% stated that their current COVERAGE does not meet their needs. (Q.3)

Forecasting 2032 **VOICE** needs revealed that fewer respondents (87% down to 82%) believe they will have sufficient capacity by 2032. This indicates some anticipate growth in voice capacity demand, even as broadband voice and data is further implemented. Respondents also anticipate some improved coverage in VOICE systems by 2032, which may also be a factor in increased capacity demand. (Q.5)

Respondents were asked to rate Coverage and Capacity of their current **BROADBAND** system and to forecast Coverage and Capacity of their **BROADBAND** systems in 2032.

Current CAPACITY for **BROADBAND** was rated as mostly meeting the respondent's needs (79%). Current COVERAGE was rated as a problem as only 57% stated that their current COVERAGE meets their needs. (Q.4)

Forecasting to 2032, **BROADBAND** needs revealed a slight reduction (79% down to 74%) in the respondents who believe capacity will be sufficient. The survey shows a 10% increase in respondents (67% up from 57%) who believe coverage will be sufficient by 2032.

SURGE DEMAND

Respondents were asked to estimate the current demand for voice and data communications when major incidents occur. The increase values were set at ranges of 10-30%, 31-60%, 61-90%, and above 90%. Most responses indicated a 31-60% increase in **VOICE** traffic and a 10-30% increase in **DATA** traffic. (Q.16)

They were then asked to estimate whether that surge would further increase in 2032. Approximately three quarters of respondents anticipate an increase in **VOICE** traffic surges with almost all respondents anticipating an increase in DATA traffic surges by 2032. (Q.17)

REDUNDANCY

Respondents were asked to rate the value of redundancy in their communications systems. About three-fourths of the respondents indicated redundancy was more critical in their voice systems (75%) and control channels (72%), compared to about half the respondents for public safety broadband systems (51%).

BROADBAND EFFECT ON VOICE

Respondents were asked if **VOICE** traffic would increase, decrease, or remain the same due to the expanded use of Broadband systems. Half of the respondents believe it will increase (42%) or stay the same (8%) with the other half believing it will decrease.

Respondents were asked if **DATA** traffic would increase, decrease, or remain the same due to the expanded use of Broadband systems. None indicated it would decrease. Over 90% believe it will increase.

INTEROPERABILITY

Respondents were asked to indicate the roadblocks they face for interoperable communications and multiple answers were allowed. (Q.20) The vast majority believed funding was the greatest roadblock to interoperability. It is possible that many of those indicating that funding was a roadblock also answered that training, obsolescence, and infrastructure were roadblocks because of funding. Many roadblocks can be addressed once adequate resources are dedicated to resolving them.

When asked if their agency had plans to address interoperability roadblocks, the greatest number of responses (74) indicated additional funding is planned and 66 responses indicated additional training is planned.

DATA INTEROPERABILITY

Respondents were asked how important interoperability is when it comes to certain data applications, with all results provided in this section rated as critical or important. The strongest responses indicated that Computer Aided Dispatch (CAD) interoperability is critical or important (88%), with map-based application interoperability close behind (87%). Messaging is rated critical or important at 76%, records management at 73%, Automatic Vehicle Location (AVL) at 69%, and Video at 64%. The importance of data interoperability for Robotics was rated as critical or important by only 38%. (Q.1)

When asked if there were other applications that were critical for data interoperability, respondents clearly want their voice applications to be interoperable. (Q.2)

VOICE

Responders were asked to forecast their agency's narrowband voice channel needs in 2032. 88.8% answered that their channel needs would either increase or remain the same. (Q.1)

They were then asked to indicate which technology is utilized for voice. Many responding agencies still use analog but anticipate much less analog technology utilization in 2032.

DIRECT DEVICE-TO-DEVICE (VOICE)

Respondents were asked if it was important to their operation to maintain direct device-to-device voice capabilities and 94.7% answered yes.

ENCRYPTION

Respondents were asked if they used encryption on their voice channels. 61.5% utilize encryption on Special Event channels, 57.7% on Normal channels, and 34.6% use encryption on Interoperability channels. (Q.4) AES-256 encryption was the dominant encryption algorithm.

IN-BUILDING VOICE

Respondents were polled on whether their jurisdiction has ordinances, building codes, etc. that require in-building public safety communications coverage in new and/or existing buildings. 71% require it in new construction while less than half require it in existing construction. (Q.6)

Respondents were asked how confident or concerned they were about their agency's ability to communicate by voice inside all buildings. About the same number were "somewhat confident" (30.1%) as were those "somewhat concerned" (32.3%). (Q.7)

DATA

Respondents were given a list of data applications and asked if they currently use or plan to use them by 2032 (Q.1). It is accepted that the values represent future use as added to current use. They were then asked which data applications would impact their operations if that capability was lost (#3). The applications that appeared to have the least operational impact if lost was Robotics (5%), High-Resolution Photos (9%), High-Resolution Video (7%), and Low-Resolution Video (6%).

IN-BUILDING BROADBAND

Respondents were asked about the importance of in-building broadband coverage across all data applications they use. Based on the respondent's ratings of critical or important, it is clear that indoor broadband coverage is a capability required for the listed applications. (Q.5)

FUTURE BROADBAND APPLICATIONS/DEVICES

Predicting what capabilities will be available in the future is always challenging. When asked what broadband applications and devices they would desire, health data and resource tracking were most important. (Q.7)

DIRECT MODE FOR DATA

Respondents were asked if they require direct device-to-device capabilities for data applications, and 55.3% answered no.

Those who answered **YES** to direct mode broadband were mostly addressing voice over broadband as an operational requirement.

DATA PLATFORMS

Respondents were asked what platform they utilize for data applications. Again, it is accepted that the current and future values are cumulative. Although fewer participants were from Canada, the Canadian PSBN is addressed in this survey with 11 of the Canadian respondents indicating they currently use or plan to use the PIA. In the United States, survey responses indicate that public safety uses FirstNet and/or commercial broadband networks for their data applications. (Q.10)

When asked which applications their agencies run on data networks, a large portion indicate some form of Computer Aided Dispatch (CAD). (Q.11)

NARROWBAND DATA

Respondents were asked if their agency uses narrowband data networks currently and if they plan to use them in 2032. Current use was essentially split between yes and no. However, asking about the expected use of narrowband data networks in 2032 revealed a large amount of uncertainty as to its viability in the future. (Q.14)

THROUGHPUT REQUIREMENTS

Respondents were asked to forecast whether their agency will be able to provide responders' throughput requirements in 2032. 39.6% answered "No" and 53.8% said they "Don't know", which highlights the uncertainty and difficulty of planning network capacity.

VIDEO

Overall, video needs to align with live video streaming, including from alternative sources. Buffered video was not considered to be as beneficial as any form of live video streaming.

LIVE STREAM VIDEO

Respondents were asked about their anticipated use of **LIVE STREAM** video from a Communications Center to the field, field to the Communications Center, and field unit to field unit. Responses show that the opinions about **LIVE STREAM** video for each of those paths are relatively equal. About a third either agree or strongly agree that all three paths will be required.

BUFFERED VIDEO

Question #2 asked about the same paths concerning **BUFFERED** video and opinions were far less strong on the need for this.

LIVE STREAM VIDEO FROM ALTERNATIVE SOURCES

Respondents were asked about their opinion of the value of **LIVE STREAM** video from manned aerial platforms, unmanned aerial platforms, public sector cameras, private sector cameras, and robotics. Every type of video received positive responses of "strongly agree" or "agree".

TECHNOLOGY ASSESSMENT

Technology is ever-changing and constantly accelerating. Looking back to 2013, it was an era where smartphones were nascent, many cameras were still using film, and location required a clear view of the sky via GPS. Push-to-talk networks were mostly isolated from the internet and radios were simple, with no real concerns about cybersecurity. With 9/11 still dominant in the minds of first responders, the primary focus was on narrowband voice and interoperability. Spectrum and funding for the nationwide public safety broadband network (NPSBN) had only recently been authorized by Congress and NPSBN implementation was largely in the planning stage.

Fast forward to today, 2024, and the amount of technology we have in our pocket was unimaginable then. We have the ability now for a) high-speed internet in our pockets, b) cameras in our phones with quality approaching that of DSLRs, c) connection to satellites directly from some smartphones, and d) we can determine our indoor and outdoor location within a few meters. Impacting 9-1-1 calls, there is a generation that has never had a landline phone and future generations will be the same. Push-to-talk radios are now running the same software as some smartphones. These advancements all offer a significant increase in communications capabilities for the public safety community.

Unfortunately, public safety also has new challenges that must be addressed. Radio networks may have external network connections and communications networks may be shared with the public, presenting new concerns for cybersecurity. The U.S. government Cybersecurity and Infrastructure Security Agency (CISA) notes: "*As communications technologies become more and more sophisticated, so do the threat vectors posed by malicious cyber actors with the intent to disrupt public safety communications. In light of the risks and potential consequences of cyber events, CISA is focused on strengthening the security and resilience of public safety communications.*"[1]

Public Safety communications advancements involve people, not just technology. A new generation of public safety personnel is joining agencies, and this generation has increased expectations for technology, a trend expected to continue with future generations as well. New members of the public safety community see the svelte and sophistication they have in their pocket while off-duty and may not fully appreciate the requirements that mandate a larger, more bulky radio. Public safety technology needs to consider the expectations of both the users and the public they serve.

The rise in domestic terrorism and the resulting mass casualties force a distinct change in public safety response. For a variety of factors, the intensity of wildfires and other natural disasters has increased.[2] Each component is significantly different than the focus of the 2012 AFST report and highlights the challenges in predicting the technology and environment ten years from now.

To best meet the predictions, we conducted a survey to determine the future expectations from public safety. One of the inherent challenges is that while the overall public safety mission is the same between urban/suburban and rural agencies, the environment and available resources differ dramatically.

We also analyzed the results with guidance from technology experts to best categorize and expand on the expressed public safety needs. One of the inherent challenges in describing a technological future is to ground the approach in reality. Whether it's technological, regulatory, policy, or budgetary, these all factor into what new capabilities are available to public safety.

While public safety technology is the focus of this report, we must be cognizant of the technological changes in the public's hands. Advancements in consumer technology introduce new challenges but also new opportunities to better serve constituents by helping to reduce time to location and to save lives.

[1] https://www.cisa.gov/public-safety-cybersecurity

Enhancements in smartphone location capabilities provide better indoor location that can be passed to first responders, victims can use cellular smartwatches to request assistance, and satellite connectivity through a smartphone allows stranded and remote hikers to be rescued.

Technology does not come without a cost, however. The price of devices and services continue to rise as capabilities increase, and these new capabilities introduced by new devices need to be justified and funded. Agencies may struggle to meet the costs of keeping pace with the latest technology. There is also an impact on responder attention: the more technology placed on a first responder, the less the focus is placed on the human elements. Technology needs to be simple to use and not distract first responders from what and who is around them.

ENVIRONMENT

A cascade of unprecedented environmental disasters are increasing each year. Wildfires, major storms, tornados, flooding, droughts, and heatwaves stress emergency services and change the nature of response. It is estimated by the federal government that extreme weather events cost the United States about $150 billion per year.[3] The U.S. Environmental Protection Agency advises that "*Since 1983, the National Interagency Fire Center has documented an average of approximately 70,000 wildfires per year*".

The increase in the area burned leads to a stark reality for public safety. Previously untouched areas are now experiencing fire seasons, and fire seasons may become year-round conditions. The forested areas affected are so vast that it generally isn't possible to monitor everything from the ground. Therefore, space-based imagery systems in combination with strategically placed sensors may improve the potential to locate wildfires before significant damage occurs.

OTHER FACTORS

In addition to environmental changes and increased cybersecurity risks, the public safety community faces other challenges. The number of mass shootings, particularly in schools, have increased over time.[4] It is expected that this trend could continue into the next decade. These events require interoperability not just among traditional first responders but with federal authorities as well.

Public safety faces an ever-changing local, state and federal political landscape that impacts the ability for public safety to operate. While such changes may be in response to many factors, the process can create uncertainty for public safety while decisions are made and enacted.[5] Policy makers in some jurisdictions have imposed restrictions on law enforcement use of new technologies.[6] Even if these restrictions are well-intentioned, they can make the job of public safety harder to accomplish.

In summary, in 2024, public safety must effectively navigate the complex combination of new technology, changing people skills and expectations, environmental factors, increasing cybersecurity risks, and ever-changing political landscapes. This requires adaptability, training, and adequate funding.

[3] https://nca2023.globalchange.gov/

[4] Number of mass shootings in the United States between 1982 and December 2023 https://www.statista.com/statistics/811487/number-of-mass-shootings-in-the-us/

[5] For example, see Washington Post article dated February 6, 2024 regarding a recent DC crime bill under discussion. https://www.washingtonpost.com/dc-md-va/2024/02/06/dc-council-crime-bill-vote/

[6] See https://www.ncsl.org/transportation/current-unmanned-aircraft-state-law-landscape

WHAT IT COULD BE, WHAT IT SHOULD BE, OR WHAT IT WILL BE

When addressing the next ten years, there are three paths: what it could be, what it should be, or what it will be. The order of each path becomes progressively less optimistic based on the constraints within which public safety operates. Public safety must balance budgets in terms of technology and scale. This is a difficult challenge; ensuring that a system is optimized for everyday operations yet still capable of facing unforeseen disasters. To stay in business, vendors and communications providers must also be willing to target a smaller audience while being able to attain profitability on technology investments and services that meet the needs of the public safety market.

The survey results are clear that over the next ten years, public safety expects to use both LMR primarily for mission-critical voice whereas broadband service will be used primarily for data. Each type of system has its own attributes, and this does not factor in the drastic change that Satellite Communications (SatCom) will provide when Low Earth Orbit (also known as LEO) arrives. Some smartphones already have the capability to communicate directly with satellites, and this feature is expected to grow over time.

What communications system works best will depend on the agency, the operations it has, and the terrain in which it operates. Currently, a properly designed and funded LMR system provides the best coverage, reliability, and provisions for redundancy that public safety users require. However, it inherently does not have the bandwidth needed to support broadband data and can be challenging for interoperability. In turn, a network like the NPSBN or a commercial broadband system offers significantly more bandwidth to support high data speeds, simplified interoperability, and the benefit of small formfactor devices. However, universal coverage at these bandwidths is more challenging. This is because of the physics of bandwidth vs. coverage, and because smartphone-style devices operate at lower power levels than typical LMR devices.

At some point, public safety agencies may have the option or need to trade coverage for features. What is lost in power for cellular, is gained in the number of frequencies and in the number of sites. What is also gained is capability through bandwidth. LMR operates on limited bandwidth channels and therefore has limited data throughput. Video represents a unique opportunity for incident commanders to have better eyes on the situation around them, and IoT provides additional information about the surrounding area and first responders. These opportunities are not supported by LMR systems.

While communications problems certainly must be minimized, first responders typically know backup procedures to operate when there is a communications outage or coverage gap, whether they are in urban or rural environments. There needs to be faith in the personnel behind the technology that they will succeed in their task even if communication is challenging or unavailable.

One element of communications reliability is to incorporate monitoring of the communications system (LMR, cellular, or otherwise) at a user level to automatically track when issues occur and ultimately to determine the root cause of any issues experienced. Technology has advanced further than some have imagined, and capturing the most basic troubleshooting information would be a significant step forward.

Reliability is of key importance to public safety. Systems designed with public safety use in mind typically incorporate elements of redundance and resiliency. For example, systems will have backup power for the infrastructure. While it may seldom be needed, when the normal power is out due to a major storm, backup power and isolated site operations (such as site trunking) is essential in keeping public safety communications operational. While the APCO ANS 2.106.1-2019 "ANSI/APCO Public Safety Grade Site Hardening Requirements" standard exists, it is uncertain how hardened cellular sites will be in the future. For example, a transition to smaller cells located on streetlamps could create an environment in which twenty-four-hour runtime on backup power is cost-prohibitive or physically impossible. Public safety may need to advocate for backup power at cellular sites as some jurisdictions are doing.

CYBERSECURITY

Securing our nation against cyber-attacks has become one of the nation's highest priorities. Cyberattacks can have instant, wide-ranging consequences and no country, industry, community, or individual is immune. Public safety relies on communications, and the advent of wireless communications and interagency data sharing has raised concerns about the security of that critical information. Cybersecurity involves protecting information by preventing, detecting and responding to attacks.[7]

Cybersecurity risks can potentially affect every technology that public safety uses: servers, computers, network equipment, smartphones, and even modern radios. Cybersecurity threats can originate globally, and this is a paradigm shift that cannot not be taken lightly. The DHS Cybersecurity and Infrastructure Security Agency (CISA) has developed a Public Safety Communications and Cyber Resiliency Toolkit *"…to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats."*[8]

SAFECOM surveys in the past have shown that public safety is unprepared for cyberthreats that will only increase over time. In a SAFECOM survey from August 2018, 80% of agencies reported either zero funding or insufficient funding for cybersecurity, with 55% indicating zero funding whatsoever.[9] Cybersecurity extends to cloud providers as well as managed service providers. In some instances, the managed service provider was compromised; in what would have been an isolated incident now affected multiple agencies.

DEVICE CONVERGENCE

Privacy risks from smartphones and smartphone-like devices present a risk to public safety. As radios adopt smartphone operating systems, the inherent insecurities they introduce needs to be addressed. It is possible that policies already created for department smartphones can be applied to the newer radios.

POLICY AND SPECTRUM

Public Safety utilizes a variety of spectrum bands and technologies/applications to support public safety operations. The regulatory history and policies vary across these bands and technologies. Technologies continue to advance and spectrum policies continue to change. However, because of the critical nature of its communications, we expect the public safety community to embrace these changes only if/when they meet public safety operational requirements.

LAND MOBILE RADIO (LMR)

For LMR, Public Safety currently utilizes VHF Low band, VHF High band, UHF (including T-Band in some areas), and 700/800 MHz dedicated spectrum, primarily for voice operations. These bands expanded over time as public safety demands outgrew the spectrum available in a given band. As new technologies were developed to operate effectively in successively higher bands, the Federal Communications Commission (FCC) allocated additional LMR spectrum. In turn, public safety agencies license specific channels from these bands with the assistance of designated frequency coordinators and place the channels into operational use. In most of these LMR bands, the FCC also allocated subsets of channels for business-critical operations, which expanded the market for equipment in the spectrum.

[7] https://www.npstc.org/cyberSec.jsp

[8] See https://www.cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit

[9] https://www.cisa.gov/sites/default/files/publications/SNS%2520Results_FINAL_508Compliant_02112021.pdf

Technology for these LMR bands has transitioned over time from analog to digital with increased deployment of the P25 standard to enhance operability and enable interoperability. Interoperability is a key requirement for public safety, especially for major incidents or disasters when first responders from multiple agencies and jurisdictions need to communicate with one another. The deployments of statewide and regional LMR systems have enabled interoperability across multiple jurisdictions, and this directly affects the policies in place for systems. In addition, it also impacts frequency licensing.

BROADBAND

Public safety recognized that in addition to LMR, it had a growing requirement for broadband spectrum to support high speed data, imaging, video communications, and higher quality audio that LMR cannot support. Many public safety agencies use one or more commercial providers for broadband communications, and that trend is expected to continue as reliance on various data applications, imaging and video grows.

The public safety community joined together and mounted a major campaign to obtain spectrum for a Nationwide Public Safety Broadband Network (NPSBN). Just prior to the previous NPSTC AFST 2012 Report, Congress passed legislation that established spectrum and initial funding for the NPSBN and the FirstNet Authority within the Department of Commerce/NTIA to oversee the NPSBN implementation and operation. The spectrum allocated for the NPSBN is located in the 700 MHz band, adjacent to sub-bands allocated for commercial broadband, and is also available for commercial use. The legislation enabled development of a partnership approach in which public safety could benefit from the significant technology development for the broader commercial broadband market. The FirstNet Authority created by the legislation within the Department of Commerce subsequently contracted with a single commercial carrier to deploy and maintain the NPSBN.

The approach in Canada through the PSBN Innovation Alliance will use multiple carriers, and this aligns with the approach of other countries. PIA's approach will be to use multiple carriers to provide coverage to first responders throughout Canada, which will also have priority roaming on all carriers. The same 700 MHz spectrum in use by FirstNet in the United States will also be used for public safety in Canada.

In general, public safety benefits from the technology development and standardization for the overall broadband communications market. That technology development and standardization has accelerated over the years as spectrum has been made available both in North America and globally, expanding the market for commercial broadband service and technology.

4.9 GHZ

In addition to the traditional spectrum bands that support links to the end user, public safety also uses the 4.9 GHz band (4.94-4.99 GHz), primarily for fixed point-to-point and point-to-multipoint links. FCC rules for the 4.9 GHz band allow two distinct types of licenses: 1) those for fixed point-to-point and point-to-multipoint use licensed on a site-by site basis; and 2) those that authorize use of the entire band over a jurisdiction's entire area, i.e., a geographic area-wide license, to support base, mobile and temporary fixed (1 year or less) use. While geographic area-wide licenses provide some operational flexibility for which they were originally intended, they do not include sufficient information to assess spectrum usage or provide for effective frequency coordination. The FCC has concluded that the 4.9 GHz band can support additional usage and has an open proceeding to address management of the band going forward.[10] NPSTC and its member organizations, among others in the communications community, have actively participated in this ongoing multi-year proceeding.

[10] See FCC WP Docket No. 07-100.

SPECTRUM ALLOCATION GOING FORWARD

Due to the increased demand for spectrum, the Commission increasingly relies on dynamic spectrum sharing in its allocation and regulatory policy decisions. For example, these decisions include using Automated Frequency Coordination (AFC) in the 3.55-3.70 GHz band to enable licensed Citizens Broadband Radio Service (CBRS), and the implementation of several types of unlicensed Wi-Fi in the 6 GHz licensed microwave band.

Spectrum sharing decisions are often controversial: incumbents raise concerns about potential interference and problems with future system expansion while new entrants push aggressively for spectrum access. This has especially been the case at 6 GHz, where the FCC has approved multiple types of unlicensed operations and only some require the use of AFC. Simulations provided by unlicensed proponents and accepted by the FCC indicate interference will be unlikely. However, it remains to be seen whether the sharing mechanisms adopted actually prevent interference to licensed services and how expeditiously interference can be identified and mitigated if/when it does occur. As noted above, public safety is accustomed to dedicated spectrum, given its requirements for reliability and the potential impact of any interference on the safety of first responder and the public they serve. Unfortunately, it appears that from a policy perspective, additional public safety allocations going forward are unlikely. Therefore, it is imperative to maintain the allocations public safety currently has.

Public safety use of technologies and applications that support high speed data, video, telemedicine, improved situational awareness, etc. clearly must rely on broadband capacity in addition to the narrowband voice capacity that current LMR public safety allocations support. To take advantage of the significant bandwidth available commercially, existing public-private partnerships are essential and may need to be expanded. Public safety is expected to need more bandwidth both in the field and in dispatch centers. In the future, it should be possible to integrate Low Earth Orbit communications into PSAPs and possibly Emergency Services IP Networks (ESInets). Network balancing may require intelligence to ensure that the health of each network link is correctly understood and accounted for. In addition, power to the device managing the networks needs to be redundant and avoid single points of failure.

MICROWAVE

Microwave's future is complex, with the popular and already congested 6 GHz band now being accessible to Wi-Fi devices. This trend will continue for this frequency band and others are at risk as well. With the increased demands for video (such as site security) and broadband, the existing microwave links may not be sufficient in capacity.[11]

CELLULAR

Commercial operators are well into implementing and offering 5G, i.e., fifth generation broadband technology. Work in standards bodies is also underway on 6G, sixth generation technology. In general, each successive technology generation aims to provide the capabilities for increased bandwidth and new frequency bands.

Global trends may also impact first responders within North America. Public safety agencies in some other countries are adopting cellular technology as their primary form of push-to-talk and this trend is expected to continue. Successes, such as South Korea, the Faroe Islands, and Project Broadway in the European Union, demonstrate the viability of cellular for public safety communications in those areas. These deployments also include Mission Critical Services (MCS) across multiple cellular carriers. The multiple carrier approach will also be used in Canada with the PSBN Innovation Alliance (PIA) as mentioned previously.

[11] https://ipvm.com/reports/bandwidth-guide-for-video-networks

Technology exists that allows smartphones to quickly switch between carriers, even using the same SIM for both. However, this requires the technology to be approved by the carriers. Disaster situations do not differentiate between who owns what communications sites, and whatever resources are available could be used. Using multiple SIMs is one option and some public safety agencies already subscribe to two or more carriers to help enable the coverage and redundancy deemed necessary for their operations.

Network monitoring requirements could be more robust than they currently are and should include automatic user device collection. When key performance indicators (KPIs) are not being met, these incidents should automatically be flagged to be reviewed. Issues could occur with handover, coverage, capacity, and/or localized interference that may be impossible to deduce otherwise.

MISSION CRITICAL PUSH-TO-TALK (MCPTT)

Technology developments are also focusing on cellular Push-To-Talk (PTT) for the public safety market, with the standard known as Mission Critical Push-To-Talk (MCPTT). Mission Critical Push-To-Talk (MCPTT) adoption has been slower in the United States than some other areas of the world. The challenge lies in bridging Mission Critical Services (MCS) between networks in the United States, and the question is not so much technical in nature but business. A lack of MCS interoperability could fragment the use of these services and prevent adoption. The Department of Justice is addressing the challenge by adopting Over-The-Top (OTT) PTT, which may be proprietary.[12]

An additional challenge lies in key coordination for MCPTT. It is hoped that the National Law Enforcement Communications Center (NLECC) will continue to provide their crucial encryption key coordination services with MCPTT, and agencies should work with NLECC to establish this capability.

CELLULAR CHALLENGES

Challenges remain: rural coverage, direct off-network operation, and voice interoperability across multiple commercial broadband systems in the U.S. are all issues that remain to be resolved.[13] Cellular infrastructure is dependent on a network connection, except where Isolated Operations (IOPS) has been deployed. It is not possible to determine if carriers have deployed this and where, and this presents a challenge in public safety planning.

Proximity Services, also known as ProSe, Sidelink, or Device to Device, are the intended anchor for cellular public safety communication when cellular networks fail or don't exist. However, the availability of this feature has been limited to a handful of devices and has not been available in the United States.

eMBMS (Enhanced Multimedia Broadcast Multicast Service) represents a critical technology for public safety, allowing cellular messages to be "broadcast" to multiple users. While this seems obvious to those familiar in LMR as one talkgroup message should only be sent once at a site, this is not the case for cellular without eMBMS. The commercial availability of eMBMS is more limited and public safety requires it for efficient communications.

There are specific security features within the standards, such as MCSMI (Mission Critical System Migration and Interconnection), that are intended to address security concerns for Mission Critical Services interoperability. Other countries are also using multiple carriers for interoperability and redundancy reasons.

[12] https://www.criticalcommunicationsreview.com/ccr/news/101629/us-department-of-justice-selects-eschat-secure-broadband-push-to-talk

[13] See PS Docket No. 19-254 regarding a request for declaratory ruling and Notice of Proposed Rulemaking regarding interoperability on the NPSBN. https://docs.fcc.gov/public/attachments/DA-19-902A1.pdf

BRING YOUR OWN DEVICE (BYOD)

Some agencies are considering Bring Your Own Device (BYOD), and this poses significant challenges. As the agency no longer has total control of the device, there is a risk that information could be leaked based on apps installed. As an example, if a user took a photo of a crime scene (intentionally or accidentally), this could be exposed to apps that have access to the phone's photo album.

In addition, if the phone is required as evidence, the user will be without a phone for the duration. Depending on the court case, this could be a protracted amount of time. It may be possible to image the phone to avoid this issue, but this can have its own caveats.

Either due to the phone being forensically imaged or submitted as evidence, the phone's entire contents could be made available, regardless of its evidentiary value. This could expose information unrelated to the public safety case at hand that the user wants to keep private.

There are some efforts to have all of the information reside in the cloud and thus the device would not be required for evidence, but it is unclear how successful this is and may vary by jurisdiction or court case.

5G

5G has achieved a significant amount of momentum, but true 5G is still arriving. Certain cellular carriers are still fielding 5G NonStandAlone (NSA), which attaches 5G sites to an LTE (i.e. 4G) core. The explicit downside is that all of the envisioned 5G benefits are not realized. In addition, connectivity issues and delays may appear when a user is transitioned from LTE 4G to a 5G site, which occurs frequently when users need more bandwidth. When 5G StandAlone (SA) deployments are more common, the real benefits of 5G for public safety will become apparent. 5G SA offers lower latency, prioritization enhancements, and make-before-break connectivity.

6G

It is anticipated that the first deployments for 6G may occur in 2028. However, most of the RF emphasis is on frequency bands that would not be useful to public safety. Most of the 6G advancements will not directly benefit public safety and will most likely increase the cost, but there are some opportunities available.

Artificial Intelligence (AI) is intended to be used throughout 6G, providing optimizations in communication throughout the system. If it fulfills its promise, it should allow for better, faster communications, including longer distances or improved performance in poor signal conditions.

The goal of Integrated Sensing and Communication (ISAC) is to be able to sense the environment using RF waves. ISAC provides opportunities to deliver new capabilities in mass casualty and hostage scenarios, where it might be possible to determine the number of occupants within a room. In addition, it may be possible to determine smoke or sprinkler activation based on the RF measurements within a building.

CELLULAR SATELLITE COMMUNICATIONS

Some smartphones have the built-in capability to speak directly to satellites, and these have already been used to request assistance from public safety. However, there is a significant trend that unmodified smartphones can already communicate with Low Earth Orbit (LEO) satellite systems. This has already been demonstrated within the United States,[14] and carriers are starting to partner with satellite communication vendors to offer this service. Cellular phone standards are already building future

[14] https://www.businesswire.com/news/home/20220208005240/en/Lynk-Completes-Pre-Commercial-Trials-for-5th-Satellite-ahead-of-Commercial-Launch

capability within the Non-Terrestrial Network (NTN) standard.[15] For remote operations that have a clear view of the sky, this could be a significant change in operations.

LEGACY RADIO SYSTEMS

Legacy radio systems are expected to remain in operation for some time in the future due to the lower frequencies available and higher output power than cellular systems. However, there are challenges in operating these systems.

As systems have necessarily become more sophisticated, the costs of these systems have risen significantly over the past ten years, and it is more challenging for public safety to fund these systems. Personnel who are RF experts are retiring and there is a daunting challenge in replacing their decades of experience and expertise. Both of these challenges, cost and personnel, drive public safety towards creating larger solutions such as statewide systems.

Statewide systems have significant advantages as well as drawbacks, but overall, these can provide more seamless communication for public safety agencies. Challenges may exist in the overall "ownership" of the system such as how the system is maintained/operated, how to coordinate upgrades, and system funding. These are issues to be aware of and address when joining a statewide system. We expect the need to address these issues upfront will remain.

Some manufacturers are offering managed services for radio systems, and these can even include the management of statewide radio systems. This can have advantages with respect to support and access to maintenance personnel, however, the cost and ownership model may be untenable for some agencies. There is also the risk that a breach in the radio system could affect every user in the state, so cybersecurity is an increasingly important component of such systems.

With sufficient funding, a well-designed LMR system can provide public safety with the coverage, reliability, redundancy and features, such as direct off-network communications, required for public safety operability, as well as interoperability. The survey results indicate that sufficient funding is a challenge. We expect that public safety voice requirements for redundancy, reliability and direct off-network communications will result in a continued reliance on P25 systems within the United States for at least the next ten years on which this report focuses.

HANDHELD DEVICE POWER

The mission critical nature of public safety communications, the reliability required, and funding limitations on deploying sites have driven public safety to rely on devices with power higher than that typical of commercial cellular devices used by the general public. While High-Power User Equipment (HPUE) devices exist for cellular systems, this is in a limited frequency band that has a maximum allowable power of 1.25W. This challenge is exacerbated because the highest power (1.25W) is not available in handheld devices. This represents a significant step back from the 2.5-3W radios the users are accustomed to using, and there has not been any recognized progress towards extending the Occupational PTT Radio SAR limits to public safety cell phones. Lower power levels on user devices unfortunately may translate to coverage issues, especially when a first responder is necessarily located in a basement, parking garage, etc. that has a weaker network connection. For this reason, some jurisdictions require supplemental in-building coverage, but this has not been extended to cellular communications.

[15] https://www.3gpp.org/news-events/3gpp-news/5g-ntn

INTEROPERABILITY

VOICE INTEROPERABILITY

Interoperability between private organizations and public safety remains a challenge, and this may be intensified in the future. Private cellular networks are becoming more common[16] in areas such as ports,[17] refineries, factories, and mines.[18] These private networks may use their own cellular push-to-talk.[19] This presents a unique challenge where public safety cellular devices may not be able to communicate with local personnel or may not be allowed on the system at all. This is not a simple undertaking, and standards organizations should work to ensure that the standards allow for public safety personnel to communicate on a private network as required.

DATA INTEROPERABILITY

While voice has various standards (AMBE+2, AMR-WB, etc.), data does not have the same convenience. There are many different data standards, and the data contained within the standard will be completely different from one device to the next. This represents a current and significant obstacle for public safety, and this is anticipated to be exacerbated as Internet of Things (IoT) devices increase.

PERSONAL AREA NETWORKS

Wireless connectivity between local devices such as radios and wireless speaker-microphones, is referred to as a Personal Area Network (PAN). Traditionally using Bluetooth, a PAN enables connectivity that is more convenient than using traditional wires. PANs are especially useful when the user is in a situation where wires constrain essential movement, such as using Bluetooth for microphones imbedded in a firefighter's SCBA mask. Wireless allows additional convenience; however, it can also introduce new challenges. Bluetooth and Wi-Fi use unlicensed spectrum, which anyone is free to use. This presents a significant risk for interference, particularly in crowded locations.

Efforts in 2018 to introduce a public safety Bluetooth were unsuccessful because the lack of users that would use the feature and the most easily adaptable band (4.9 GHz) lacks global harmonization. However, 4.9 GHz does have overlap with at least one country, Australia.

INTERNET OF THINGS (IOT)

Internet of Things (IoT) indirectly refers to sensors, and sensors will play a much larger role in the future, whether they are specific to public safety or merely in the environment in which public safety operates. IoT could be dedicated sensors that are placed (environmental or within a building) or worn on personnel. One challenge for body-worn sensors, particularly those with cellular connections, is ensuring that the sensor is associated with the correct first responder.

Fire personnel will benefit from biometric sensors as firefighters face a significant risk of heart attacks. A 2005 NFPA study indicated that 44% of on-duty firefighter deaths were due to cardiac events.[20] Little has

[16] https://aws.amazon.com/marketplace/pp/prodview-6m7asjllevcdc#offers and https://www.globenewswire.com/news-release/2023/09/05/2737535/0/en/Private-5G-Network-Market-Size-to-Reach-USD-129-6-Billion-by-2032-CAGR-48-2-DataHorizzon-Research.html

[17] https://www.ericsson.com/en/blog/2024/3/accelerating-smart-ports

[18] https://stlpartners.com/articles/private-cellular/private-networks-use-cases-oil-gas/

[19] https://www.ericsson.com/en/blog/2023/11/private-5g-cellular

[20] https://www.cdc.gov/niosh/docs/2007-133/pdfs/2007-133.pdf

changed since then, with a 2021 study performed by researchers indicating that cardiac events were now over half. By monitoring the firefighters during the significantly stressful situation of fighting an interior fire, this would help alert an incident commander to a potentially hazardous health situation.

ROBOTS

It is also important to limit the amount of time that is required for personnel to be inside a fire structure. Properly designed robots can operate in hostile environments for longer periods than firefighters and can take additional risks. Should the structure collapse, the equipment may be damaged or destroyed, but no lives would be lost. This has been proven possible by the 2019 Notre Dame fire, in which robots were used for imagery as well as fighting the fire itself. Underwater robots can be used for underwater search and avoiding/minimizing the placement of divers. Additionally, it is also possible to use robots in HazMat environments.

The challenges for using robots for fire suppression (beyond cost) is mobility and weight. The first potential hurdle is the ability of the robot to navigate stairs and debris. Many family homes are wooden structures, and it would be a challenge to operate a robot on floors without concrete. Floors can also be compromised by fire and/or water, and a robot would be unable to determine the structural strength below it. It is expected that in the future robots will fulfill a specific role within HazMat as well as commercial structure fires.

While we do not anticipate that search and rescue in a fire structure will be performed by autonomous devices, we do anticipate methods to navigate firefighters within unknown structures and indicate the nearest exit for an evacuation. As well, the ability to approximately, but accurately determine a firefighter issuing a mayday is expected in the future.

UNCREWED AERIAL SYSTEMS (UAS)

Uncrewed Aerial Systems (UAS), often referred to as "drones", play a role in public safety that is expected to increase in the future. UAS have proven to be highly versatile in covering large amounts of area very quickly and without the added costs and other requirements inherent in deploying helicopters and fixed-wing aircraft. UAS are also capable of dropping or delivering supplies, such as automated external defibrillators (AEDs) to victims or life rafts to those trapped in dangerous waters.

Aerial search and rescue appears is a key use for UAS, but not the only type of operation that can be beneficial to public safety. At least one agency has also used "disposable" UAS to inspect HAZMAT situations, where UAS replacement is considered to be preferable to placing personnel at risk. There is also the potential for UAS to be used to improve damage assessments, and this can greatly speed up assessment operations. Unfortunately, there is a risk that UAS can be used against public safety, and this needs to be dealt with appropriately.

Public safety UAS operation is subject to Federal Aviation Administration (FAA) regulations. The FAA has developed a brochure entitled Drones in Public Safety: A Guide to Starting Operations.[21] However, drone regulation remains a challenge for public safety operations. The certification options present different obstacles for agencies as well as different liability risks. The certification approach also impacts the waivers required for operation. Beyond Visual Line of Sight (BVLOS) operations can also present challenges, though there are ways to address this. Hopefully, in the future, BVLOS operations will continue to be expanded.

[21] Drones in Public Safety: A Guide to Starting Operations (faa.gov)

SMART CITIES

The challenges with smart cities have always been establishing what a smart city is, what benefits will be provided, and who will fund them. So far, the strongest case for smart cities has been for transportation, i.e., optimizing traffic flow to minimize the environmental impact that transportation has. For first responders, this would allow for better movement of emergency vehicles in crowded streets. Some arguments have been made for monitoring the electrical power grid and these may also have merit. From a surveillance camera standpoint, smart cities may be able to identify crimes in progress, identify victims and perpetrators, and aid in the apprehension of perpetrators.

Whatever the form that smart cities take, care must be taken to ensure that a surveillance state is not established and minimizing the new security vulnerabilities being introduced. Good design should incorporate mechanisms to prevent unintentional internet access to the devices, prevent physical access to the device itself, and have password/reset restrictions when directly accessed.

SMART BUILDINGS

Efforts have been made to standardize smart buildings, but this remains a challenge. HVAC systems, indoor communication systems, fire suppression systems, electrical systems, surveillance cameras, elevator systems, and occupancy sensors all have different interfaces or may not have any external interfaces at all. There is no overall standard and certification that has developed (though examples like ANSI/BICSI 007-2020 and SPIRE Smart Buildings Assessment do exist), and the rate of deployment will take some time that will extend beyond a decade. These systems must also factor in cybersecurity concerns.

Smart buildings hold the potential to allow fire personnel to determine nuisance alarms from real fires, the exact location and extent of the fire, potential areas where victims may be trapped, and the current occupancy. HVAC control would aid in minimizing the amount of new oxygen flowing to an interior fire.

DISPATCH CENTERS

The role of dispatch centers varies by agency, but the dispatch center is typically the constituent's interface to public safety. Public safety needs to optimize interactions between the field and the dispatch center, particularly with the exponential increase of information over the next decade. Dispatch centers can focus on the flow of information, triage, and share with first responders, thereby letting the first responders focus on the situation immediately around them.

As technology improves, the amount of information available to dispatch centers dramatically increases. However, the bandwidth requirements at a dispatch center are typically much lower than what would be necessary to consume all of the information. Even if all the information could be aggregated, it would not be possible for dispatch center personnel to handle the massive influx of information. This is an ideal situation for Artificial Intelligence (AI) or Machine Learning (ML) to automatically triage external information that flows into the dispatch center. One caveat, however, is that the information presented will steer someone towards a particular decision.

It is expected that Mission Critical Push-To-Talk (MCPTT) adoption will occur over the next ten years. MCPTT integration into the dispatch center seems simplistic on the surface but becomes more complicated with redundancy. If unicast audio routing is used, the amount of bandwidth required becomes significantly higher than expected. This is because the audio for each talkgroup is being sent individually to each dispatch position. As an example, if ten console positions are listening to forty active talkgroups, there are four hundred simultaneous audio streams, even if the console position has most of them muted.

If cellular redundancy is intended, this has its own benefits and challenges. If each device has a SIM card, then the dispatch center has to have adequate cellular coverage in the dispatch center room. Cellular sites must also have the capacity to handle the dispatch center's traffic in addition to normal users. IP spaces that the dispatch centers use need to avoid overlapping with the cellular network's assigned IP range.

9-1-1 location accuracy is expected to improve, particularly in the Z-Axis (vertical direction). This improvement is critical in situations where constituents do not have landline phones, particularly in high-rise buildings. Location update rates are critical when the situation is dynamic.

NG9-1-1 and ESInet adoption rates are expected to continue, with regional deployments and statewide deployments being the predominant path forward. The ESInet made the architecture a lot easier, particularly for call transfers, and this will improve interoperability. There is also the possibility of falling back to the ESInet if other networks fail. However, the large number of upgrades required to maintain the ESInet has been surprising to some agencies.

One trend that appeared during COVID is remote call-taking, and this may continue over the next decade. Remote call-taking is possible due to the number of call-taking applications that are either hosted in the cloud or with internet access. A computer at home would access the internal network (for example, by using a VPN) and log into the appropriate application. From there, it would be essentially the same as being in the dispatch center itself, except for the element of face-to-face human interaction. This is beneficial for non-emergency call-taking or surge call-taking but has caveats.

One concern is that access to the dispatch center is restricted but access within a home is not. There is the distinct possibility (even with using headsets) that someone in the household will hear Personally Identifiable Information (PII). The reliability of the call-taking equipment is dependent on the reliability of the call-taker's home internet, which will certainly have different Service Level Agreements (SLAs) than the dispatch center itself. While the call-taker will possibly have higher bandwidth available to them, the reliability will most likely be less than in the dispatch center and performance may not be monitored. And as usual, cybersecurity is another significant concern, and multifactor authentication is required.

NG9-1-1

Respondents were asked if Next Generation 911 will drive broadband Data needs by 2032, and 80.5% answered yes.

GIS

GIS solutions will become more complex in the future, requiring additional layers to display additional information. The opinion has been consistently shared that GIS applications are not meeting the needs of public safety, and this level of dissatisfaction is expected to continue.

Creating a model of a city or area (digital twins) offers promises of additional features, but most of these have not been realized. Some areas of improvement involve urban planning and traffic flow, and these could be extended into evacuation models. Digital twins, however, are expensive to create and expensive to maintain.

ADVANCED TECHNOLOGY

The next ten years will see the largest metamorphosis in history relative to computing power, use of the cloud in more efficient ways, new types of detection and mitigation of cybersecurity incursions as many of these systems are IP-based and connected to external networks, and the advent of quantum computing.

CLOUD AND EDGE COMPUTING

The shift to the cloud has been underway for some time, and this trend is expected to continue for the next ten years. One concept that has existed for years is the idea of Edge Computing with the goal of having more intelligence in the end device. This intelligence would allow the device to perform more complex operations without having to send data to the cloud.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Whether it's actually Artificial Intelligence versus Machine Learning (ML) is a debate for a different document, but the two are pervasive in technology and culture. AI and ML are prevalent in our everyday lives: whether it's predicting our next word in a text message, assisting in our search engines, translating languages, or responding to writing prompts, AI and ML are already in our pockets. The main difference is that these applications typically aren't life or death.

What happens when AI makes a mistake versus a human being is a complex question. Lives could be lost due to AI/ML decisions but lives also are likely to be saved. However, this is no different from human decisions, and how public safety determines which is preferable is a matter of policy. Public safety agencies will need to understand the liability aspects that deploying AI/ML can have in life-threatening situations.

AI and ML are already being used for public safety, and this is expected to increase over the next decade. There is also a specific need within public safety for the AI/ML to be able to articulate how the decision was reached; blind faith in the capabilities is not possible. There are many aspects required to utilize AI and ML properly, and there are instances where it has had a negative impact on public safety and/or the constituents. The focus will be on three aspects: data, reliability, and interpretability.

Data samples are the single most important aspect for AI/ML and books have been written about the impacts on constituents. Data samples that have issues, such as being incomplete, having biases built into them, or not correctly labeled, can all make the AI/ML useless at best or hazardous at worst.

Reliability is fairly straightforward in that AI/ML needs to make the right predictions consistently and for the right reasons. One challenge that AI/ML in particular faces is that typically the failures that occur are not gradual but sudden. In addition, it can fail without warning and be unclear as to why it failed.

Interpretability is the ability to understand how the AI/ML came to its decision. This is a significant obstacle, as most AI/ML companies who care about the end result and not about how it got there. As well, the path taken by the AI/ML is considered Intellectual Property (IP) and may be under Non-Disclosure Agreement (NDA) or completely unavailable. While we hope that AI/ML will become more transparent in the next decade, that may be unlikely. However, public safety agencies need to be aware how and why AI/ML decisions are reached to interpret the suitability of their use in life-saving applications.

AUGMENTED REALITY AND VIRTUAL REALITY

As demonstrated by the NIST Public Safety Communications Research (PSCR) challenges and efforts, Augmented Reality (AR), and by extension, Virtual Reality (VR) can play a role in improving public safety training and operations.

Augmented reality takes the environment around you and enhances it. An example is being able to see a room-sized map and interact with it for mass casualty and wildfire scenarios. Also, heads-up displays for firefighters inside a burning building can provide contextual clues as to the nearest exit, remaining oxygen, firefighters in distress, and other vital information.

Virtual reality allows for training scenarios that would not be possible due to hazardous or unusual conditions. An excellent example is in hazardous materials (HAZMAT) situations or allowing personnel to quickly change between different "physical" environments. There are limitations to virtual reality, notably the inability to interact with a physical environment and the challenges of incorporating multiple personnel in the training. Some of these challenges will be addressed through VR, and some will be addressed through AR.

IN CLOSING

In this document, NPSTC has strived to be as comprehensive as possible, given the resources available. However, it is not possible to cover everything. There are some technologies and features that are not covered, such as Mobile Device Management (MDM),[22] Virtual Private Networks (VPNs),[23] and user credentialing.[24] These are important topics, and they have been extensively covered by the National Institute of Standards and Technology (NIST).

When looking back ten years, the idea that a standard smartphone in your pocket could have satellite connectivity sounded like science fiction. Yet, there are millions of people in the United States and Canada that have this. Such is the rapid pace that technology provides, and there may be concepts that have not been dreamed of that will drastically alter the communications landscape after this paper is published.

Public safety should be able to adapt to these paradigm shifts and embrace them to provide the best level of service to their constituents. This requires proper policy, proper funding, and a proper frame of mind. These are all significant challenges, but something that has not changed over time is the ability for public safety to adapt to new technology and operational requirements.

ACKNOWLEDGEMENT

We want to thank the following who made this project and resulting report possible:

- NPSTC Governing Board and PIA Board members for their overall vision and support in launching the AFST project;
- Chief John Lenihan (ret.) for his leadership and dedication in chairing the AFST project;
- Tracy Ayoung, Halton Regional Police Service (Canada) and Ronni Gibson, Peel Regional Police Service (Canada) for their expertise and dedication in survey development, survey result documentation, and overall project support;
- Ryan Poltermann, Chair NPSTC LMR/LTE Working Group for technology expertise;
- Don Root, Chair NPSTC Spectrum Management Committee and Stu Overby, NPSTC Support for spectrum expertise;
- The public safety representatives who responded to the survey and public safety review; and
- Public Safety participants from the NPSTC Broadband Technology, Interoperability and Spectrum Management committees and from PIA membership who provided advice during the project.

NPSTC and PIA are grateful for the dedicated involvement of the greater public safety community in the AFST initiative. We hope this report will be helpful as public safety agencies look to enhance essential communications tools to help meet the increasing and challenging demands they face in both day-to-day operations and when catastrophic events occur.

Regards,

Marilyn Ward, NPSTC Executive Director
Bill Payne, Halton Regional Police Service and PIA Representative
Phil Crnko, Halton Regional Police Service

[22] https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise-0

[23] https://www.nist.gov/publications/guide-ipsec-vpns

[24] https://www.nist.gov/identity-access-management/identity-and-access-management-roadmap