PRIORITY
Criminal Justice
NEEDS INITIATIVE
A project of the RAND Corporation,
the Police Executive Research Forum,
RTI International, and the University of Denver

Using Future Broadband Communications Technologies to Strengthen Law Enforcement

John S. Hollywood, Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson

Forthcoming broadband communications technologies could provide dramatically increased capabilities for law enforcement. In September 2015, the RAND Corporation convened an expert panel for the National Institute of Justice (NIJ) to discuss how law enforcement can best leverage future communications capabilities anticipated to be fielded over the next 10 to 15 years while mitigating potential risks. The Broadband Communications Workshop assembled 41 experts on both law enforcement operations and broadband technologies, and collectively identified 68 needs for technology initiatives, including both technical and nonmateriel requirements. The top ten needs identified at the workshop are listed below.

The most prominent theme of the workshop was supporting the emergence of a future broadband network in which

Top Ten Needs for Law Enforcement Broadband Communications

1. Provide agencies with guidance on how to acquire, manage, and use mixtures of communications networks technologies.
2. Research smart software agents for officers in the field to help them get info they need while avoiding information overload.
3. Explore the use of tethered unmanned aerial systems (UASs) to support rural communications and other areas that need additional communications.
4. Develop roles for people who specialize in data management of video and other high-volume law enforcement data.
5. Develop new models for general authentication of devices onto a network more like the domain name server in computing. Design devices that find the resources that the device needs to do what it wants to do.
6. Develop processes (including training/staffing), automation filtering and tools, and procedures to help public safety answering point employees prioritize incoming data and use data to support operations and avoid information overload.
7. Develop better ways to do user authentication—making it easy for individual users, for example, such that if a public safety officer leaves their device behind it is locked, but individuals from other agencies could still access it.
8. Develop concepts, policies, and procedures for mutual aid networks in a post land-mobile-radio/FirstNet/broadband era. Need to define the common roles, responsibilities, associated services and information needs, and log-on (authentication and granted permission) capabilities.
9. Research tools and methods on managing hybrid networks that include wired, commercial broadband, FirstNet, and existing infrastructure components.
10. Solve the federated identity management problem to allow authentication of one public safety person with a device to connect to a different network—navigating the challenges posed by local control. This will require a governance model that can make these decisions and get the message out to the individual departments. Need to develop an equivalent of a certificate authority for authentication for public safety communications.

law enforcement users will be able to seamlessly and securely communicate over whatever local point of access is the best fit at any specific location, time, and situation. The second major theme dealt with being able to filter, prioritize, and make sense out of all the new data sent over this network. A common concern was the danger of information overload and how to manage and curate information to make it most useful for various areas of law enforcement, ranging from officers in the field to operations centers and public safety answering points. Specific needs in support of these themes included architectural development, developing guidance for agencies on acquiring, managing, and using new technologies, and conducting research and development on a range of technologies related to bringing about the future hybrid networks and information prioritization.

INTRODUCTION

Over the past 25 years, the mobile data computer (whether in original mounted laptop or newer smartphone and tablet form factors) and the information it provides has been the principal new technology in law enforcement field operations. It has provided the officer greater situational awareness and intelligence. With the exception of the electronic control device (popularly known as a Taser™) and other less-lethal weapons, little else has changed fundamentally in law enforcement technology: Vehicles, uniforms, protective gear, protective devices, and less lethal technology have improved, but incrementally. Similarly, the major technology changes to operations centers and public safety answering points (PSAPs—the call centers that answer emergency calls for service) have been computer displays and the information they provide.

Practitioners we have worked with in both interviews and focus groups have consistently focused on the importance of getting and using key information to furthering law enforcement objectives. In prior studies to identify and prioritize criminal justice technology needs, needs for sharing and effectively using information have been dominant themes, constituting large shares of the highest-priority needs identified across multiple studies. In perhaps the most notable case, the principal positive conceptualization of law enforcement's future during a futuring workshop was labeled "Network Centric Policing" (Silberglitt et al., 2015).

Sharing and using information requires physically getting the information, which in turn requires a communications network capable of transmitting that information. Requirements for transmitting data are growing all the time—whereas 25 years ago the focus was almost exclusively on voice communications, today the focus is on electronic data, ranging from life-critical information about persons and locations of interest to vehicle tracking data. Tomorrow, communications networks will have to handle ever-growing amounts of data from a vast array of sensors that are part of the emerging Internet of Things. Perhaps the biggest bandwidth demands will be to transport large volumes of video footage all over field and operational broadband networks, ranging from officers' body-worn cameras to bystanders' smartphone footage uploaded as part of 911 phone calls to commercial security camera footage.

To assess how emerging broadband communications technologies might improve criminal justice capabilities over the long term (10 to 15 years from now), the NIJ asked RAND to support an expert workshop as part of the Priority Criminal Justice Needs Initiative (PCJNI). The PCJNI is an NIJ-funded initiative intended to promote innovation in the U.S. criminal justice system by assessing and prioritizing its technology-related needs. As will be discussed below, this workshop responds to a theme of earlier PCJNI studies commonly calling for improvements to the sharing and use of information across

> The most prominent theme of the workshop was supporting the emergence of a future broadband network in which law enforcement users will be able to seamlessly and securely communicate over whatever local point of access is the best fit at any specific location, time, and situation.

law enforcement, which in turn imply needs for improvements to the communications networks carrying that information.

In all, 41 experts on both law enforcement operations and broadband technologies participated in the conference (a full list is provided at the end of this document). They included 12 law enforcement practitioners, 12 commercial representatives, 8 academic researchers, and 9 federal representatives (government and contract personnel).

The time frame of the workshop covered technologies and deployments scheduled to come on line from 5 to 15 years from now. Given the long timelines for fully fielding communications infrastructure, this time frame roughly corresponds to examining technologies in development over the next 3 to 5 years that are expected to be fielded in the following decade. Thus, the panel talked about how law enforcement might be supported once the first increments of FirstNet, fifth-generation (5G) mobile broadband, and other key technologies currently on the "drawing board" have been fielded. (FirstNet is a government-funded initiative to build a dedicated, interoperable broadband network for first responders, using a combination of commercial broadband allocated to public safety use, construction of dedicated broadband—especially in rural areas with limited wireless coverage—and satellite communications.) NIJ has a strong interest in getting beyond "next shift/next purchase" communications issues and helping shape law enforcement communications in the 2020s. The key objective of the workshop is to inform key science and technology (S&T) development and deployment efforts, with the results and this report intended to

- inform practitioners about developments on broadband technology expected to be fielded 10 to 15 years from now that they should be able to leverage, and describe what steps will need to be taken by the Department of Justice and other federal sponsors, developers, and agencies to bring about operational improvements from the new technologies.
- inform technology developers about both operational shortfalls with existing equipment and perceived opportunities and risks with current technology trends, so that developers might better address operational needs.
- inform federal and other funders about outstanding needs to leverage emerging broadband technologies to improve law enforcement.

Previously Identified Needs for Information and Communications

RAND's prior studies on law enforcement technology needs under the PCJNI (Goodison, Davis, and Jackson, 2015; Hollywood et al., 2015a, 2015b; Hollywood and Winkelman, 2015; and Silberglitt et al., 2015) usually did not talk directly about broadband communications network requirements. However, the studies identified a number of top-priority needs for information and communications that place significant demands on future broadband networks. These can be divided into four overarching categories:

- **Communications from the field.** Maintain awareness of officers in the field, especially during major incident response. This includes tracking units' location and status and getting messages to and from them. In addition to routine operations, one of the highest-priority needs identified was for deployable tracking systems that would be issued and used during major incident responses.
- **Communications to the field.** Provide officers with tailored information displays (also referred to as "situational awareness" or "common operational picture" needs), ideally showing officers what they need to know across the range of law enforcement operations.
  - Specifically includes displays for mobile systems, including apps for smartphones and tablets, as well as operation center displays.
  - Displays need to support both day-to-day operations and major incident management.
  - Displays should include maps, map annotations showing crime analysis findings (hot spots, persons of interest, etc.), automated alerts, other "data mashups," responses to in-field queries, and mechanisms to ease officers' reporting.
  - The displays should be tailored to officers' current information needs. This includes having updates tailored to officers' specific locations, which requires bandwidth for location tracking.
- **Sensor data.** Includes video, biometrics, and health data.
  - Near-real-time video feeds from deployable closed-circuit TV (CCTV) systems. The studies called for a relatively small number of deployed cameras in support of specific operations, *not* a general video surveillance network.
  - Exchanging biometric data (fingerprints, facial photos) and analysis results to positively identify contacts in the

field, with time from collection to response ideally less than one minute.
  - Monitoring health telemetry data, sending alerts when an officer shows signs of high fatigue, high stress, or a serious health condition.
- **General infrastructure.** The studies identified some high-priority needs related directly to communications infrastructure:
  - Improve the communications infrastructure supporting law enforcement, in general. (The specific need referenced did not go into more detail than this.)
  - Lower communications technology lifecycle costs, specifically bandwidth costs.
  - Provide greater bandwidth. Here, "sufficient bandwidth" has been described as "enough so that officers in the field can exchange whatever they need with minimal lag time."
  - Have interoperable radios that permit communications across agencies; this may need to include interoperability with fire and emergency medical services (EMS), as well.

The specific needs contributing to the above summary are in the studies listed above. To provide operational context beyond these general needs, Hollywood and Winkelman (2015) present figures showing information exchanges needed to support specific types of law enforcement operations. We can further consolidate the above discussion into needs for future broadband networks to be able to transmit the following types of information:

- Voice communications cutting across multiple agencies simultaneously.
- Tracking data for law enforcement vehicles and personnel, updated regularly (at least every few minutes plus every time the vehicle or person moves a specified distance).
- Locations of incidents and supporting descriptive information, updated as those incidents occur (in near real time).
- Overlays for map displays that describe crime analysis results, such as crime clusters, crime densities, or hot spots, transmitted rapidly enough to avoid delaying officers' operations.
- Pages of images (photos, maps) and text reflecting results of queries about people, vehicles, or buildings, transmitted rapidly enough to avoid an officer having to wait for more than a few moments to carry out an enforcement action.
- Health telemetry data, transmitted specifically when on-person sensors indicate a potential problem; must be transmitted in near real time.
- Biometric data needed to identify a person; transmitting that data plus receiving a response with results should not take more than a minute in total.
- Live transmission of a "small" number of high-definition video feeds simultaneously.

NIJ and RAND staff identified a set of communications technologies that might enter wide use over the next 10 to 15 years.

An Initial Set of Emerging Technologies

To provide the workshop with a set of initial ideas for technologies to discuss, NIJ and RAND staff identified a set of communications technologies that might enter wide use over the next 10 to 15 years:

- FirstNet, which, according to the FirstNet.gov website, "has been obligated by Congress to take all actions necessary to ensure the building, deployment and operation of the nationwide public safety broadband network." It leverages two noncontiguous bands of spectrum (for a total of 20 MHz) in the 700 MHz range (D-block/Band 14: 763–775 MHz and 793–805 MHz). Current focus is on supporting incident and disaster response. Kennedy (2015) and First Responder Network Authority (2015a) provide recent updates on FirstNet; Federal Communications Commission (2016) describes the D-block spectrum allocation.
- 5G, the next major rollout of broadband mobile technology standards. (The current standards applying to most fielded mobile devices are 4G/Long Term Evolution [LTE]). Planning documents for 5G indicate support for order-of-magnitude improvements in total data volumes, connected

devices, bandwidth seen by individual users, and battery life. They are also scheduled to support push-to-talk and multicast. Next Generation Mobile Networks Alliance (2015) and Rinqvist (2015) provide perspectives on what is expected under the 5G umbrella.
- Datacasting uses TV broadcast signals as the transport of data and has all the intrinsic properties of using TV transmitters. NIJ has written about datacasting (National Law Enforcement and Corrections Technology Center, 2012).
- Improving the use of spectrum, including:
  - Making better use of *white space*, which is spectrum nominally allocated for broadcast television that is going unused in a particular area. The Federal Communications Commission has set up rules allowing the use of white space spectrum (Federal Communications Commission, 2015).
  - Pushing broadband to new bands. As one example, recent research has looked at spectrum in the 0.1 terahertz and higher frequency ranges (Akyildiz, Jornet, and Han, 2014), which makes it feasible to support data flows of terabits per second, albeit with substantial physical challenges.
  - Improved spectrum management tools, notably systems (including devices themselves) that can perform dynamic spectrum management (see, for example, Akyildiz et al., 2006). As example technologies, this category might include improving analytic methods for predicting communications requirements as well as developing apps that can prioritize existing bandwidth in near real time.
- Use of UASs as communications relays. Tozer and Grace (2001), discuss high-altitude relays; Olewitz (2015) reports on a more recent ultralight tethered UAS that can act as a local area relay, with the tether providing persistent power that can keep the UAS in the air for long periods of time.
- Improvements to satellite communications. Minoli (2015) provides a recent survey.
- Improvements and improved uses of tropospheric scatter communications, which, as the name suggests, bounce radio waves off of the impedance discontinuities in the troposphere over longer distances. Monsen (2003) provides a survey.
- Mobile ad-hoc networks, in which mobile vehicles collectively relay messages. Perkins (2008) provides a survey.
- Leveraging personal area networks and very small network cells. Chandrasekhar, Andrews, and Gatherer (2008) provide a survey.
- Freespace optical, which uses lasers to transmit data at extremely high speeds (up to Gigabits/second) through the air. Chan (2006) provides a survey.
- Software-defined radios and software-defined networks, which allow for making certain types of upgrades of communications equipment via software updates, rather than having to upgrade or replace hardware. They can also permit dynamically changing communications standards in use to match a particular operational context. Sezer et al. (2013) provide a survey.

These were intended simply as initial thought-provoking ideas, and were not meant to be a complete list of technologies considered.

Methodology

Prior to the workshop, panelists received a read-ahead that:

- Reviewed the information sharing, analysis, and use needs from earlier workshops that are driving the need (same text presented in the “Previously Identified Needs” section).
- Reviewed a set of initial ideas for technologies to consider at the workshop (same text presented in the “Initial Set of Emerging Technologies” section).
- Asked them to identify problems with current communications technologies, upcoming technological opportunities that might be leveraged, and potential solutions to problems. We used the resulting responses to identify initial topics for discussion at the conference.

Because of the size of the panel, on the first day the group was split into two randomly selected breakout groups to discuss issues and identify corresponding S&T needs independently. To organize the discussions of the breakout groups, we divided broadband communications issues and problems and corresponding ideas for innovation into four broad categories:

- **Physical layer**—hardware/wire/radios and antennas employed to build the network. Includes devices, radios, antennas, communications towers, and radio spectrum.
- **Network layer**—tools/standards for sharing and securing data between hosts. Includes both terrestrial communications and satellite communications standards such as 4G/

LTE, 5G, legacy waveforms, and Internet Protocol (IP) standards.

- **Presentation layer**—tools and standards for sharing and securing data elements between applications across the network. Includes identity credentials, access management, other security measures, and network management functions.
- **Operational considerations**—cutting across the technical layers, these are operational challenges for efficient and effective use of broadband communications technologies that need to be addressed.

These collectively provide for transporting data between parties and applications that need them. We were interested in both technology issues as well as governance/policy and acquisition/business model issues in each area.

These layers do not cover information technologies for interpreting, analyzing, and employing the data in operational contexts, or data-sharing policies and governance. Information sharing, analysis, and use needs were discussed and prioritized in earlier workshops (and summarized for the panelists in the preconference read-ahead), as noted above.

These four categories were used to organize the discussion at the workshop. The first breakout group discussion examined operational considerations for broadband. During this session, panelists reviewed the top needs from prior work that placed demands on broadband and identified additional operational issues and resulting needs for the broadband communications infrastructure.

The next breakout group discussions concerned the physical, networking, and presentation layers, which were conducted a bit differently. Prior to the workshop, participants received a questionnaire that asked them to respond to the following questions for the physical, network, and presentation layers:

1. What problems or issues do you see with [layer technologies], and how will they impact law enforcement operations if not addressed?
2. Are there specific technological opportunities at the [layer] that law enforcement communications need to leverage, looking forward 10 to 15 years?
3. What potential solutions do you see to the [layer] problems or issues?

The responses were consolidated and converted into bullets that were presented at the start of each discussion as problems or opportunities that might warrant specific S&T needs. Panelists were then invited to provide more comments on the initial list of problems and opportunities, develop corresponding S&T needs, and identify additional problems and opportunities.

On the second day, the full panel reviewed slides detailing common themes about problems and opportunities and was invited to identify additional themes and needs that appeared to have been missed previously. Workshop participants then filled out an online questionnaire to prioritize the needs generated over the course of the workshop. Participants also had the opportunity to write comments as to why they rated a need as they did. Thirty-three participants completed the ratings questionnaire.

The technical details of the prioritization are described in Appendix B (available at www.rand.org/t/RR1462). In brief, needs were prioritized based on their expected value, which combines assessments of how much value a solution to each need might be to law enforcement, how technically feasible developing a solution is, and how operationally feasible developing a solution is. We then used the expected value scores to divide the needs into one of three categories: Tier 1 (high priority), Tier 2 (medium priority), and Tier 3 (lowest priority). Several weeks after the workshop, panelists had the opportunity to take a second online questionnaire. This questionnaire showed participants the current priority tier for each need, along with the comments that had been written for each need, and offered participants the opportunity to vote needs into higher or lower tiers based on their review of the comments. Twelve panelists participated in the second questionnaire.

RESULTS: BROADBAND COMMUNICATIONS NEEDS

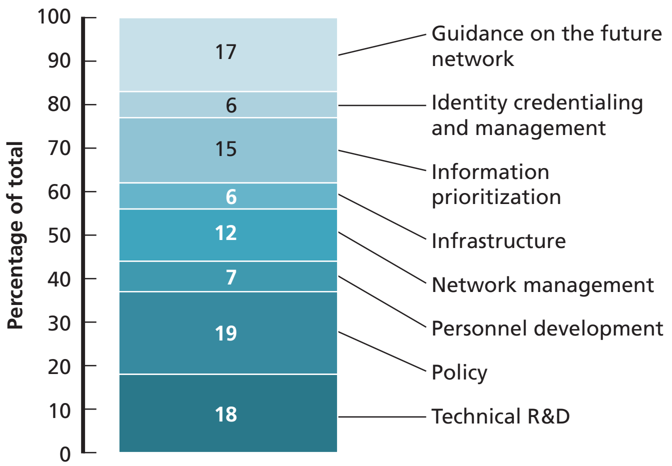
The panel generated and prioritized a total of 68 discrete needs. The needs could be subdivided into eight broad technology areas:

- Providing guidance on how to manage future broadband communications networks.
- Identity, credentialing, and access management (ICAM) for the future network.
- Enhancing communications infrastructure.
- Tools and methods to support prioritizing the large volumes of information expected over future communications networks.
- Network management tools and methods.
- Developing personnel with the roles and skills needed to manage future broadband communications networks.

- Policy needed to govern the future network.
- Other technical research and development.

Figure 1 shows the proportion of needs in each technology area. As shown, the largest numbers of needs had to do with providing guidance, prioritizing information, policy, and technical research and development (R&D). The latter covered a large set of technology areas on topics ranging from improving antennas to improving radio battery life to developing radios that can run on both legacy land mobile radio and forthcoming digital broadband networks. In general, however, the needs were pretty well distributed across the range of broadband-related technology topics; there were no truly dominant topics of discussion.

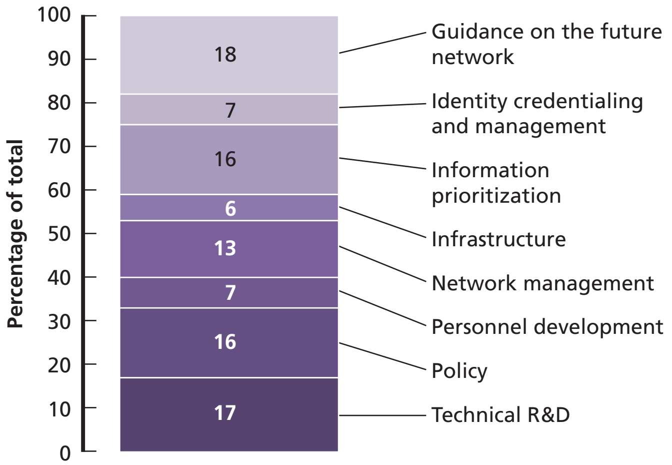
Figure 1: Proportion of Needs by Technology Area



NOTE: 68 needs in total.

RAND *RR1462-1*

Figure 2: Proportion of Needs by Technology Area, Weighted by Priority



NOTE: 68 needs in total.

RAND *RR1462-2*

Figure 2 shows the share of needs in each technology area weighted by priority. As shown, in this study the weighted shares changed little in comparison to the unweighted shares. With the exception of a three-point reduction for policy-related needs, implying that policy needs tended to be down-weighted by panelists, no change between unweighted and weighted shares was more than a single percentage point.

Table 1 shows all 19 of the top-ranked, Tier 1 needs from the workshop. Needs are shown by technology area. We present the complete set of needs from the workshop in Appendix A (available at www.rand.org/t/RR1462). For each need, we show the problem to be solved ("Problem") and the call for a specific solution ("Need)." Note that some operational problems are addressed by multiple specific needs, meaning that some problem descriptions are repeated multiple times. Except for copyediting, all problems and needs are written exactly as they were expressed during the workshop.

DISCUSSION

Two overarching themes emerged from the top needs from the Broadband Communications Workshop. The first involves supporting the emergence of a future network environment in which devices can use multiple types of communications links and in which it will be possible to manage networks dynamically to best meet operational needs. The second involves improving users' abilities to understand the torrents of information expected to be transmitted over that network. In addition to the themes emerging from the specific broadband needs, the panelists also provided insights on needs for information and communications capabilities that future broadband networks will need to support.

Below, we first discuss these needed information and communications capabilities, as they provide additional context for future broadband networks. We then consider the themes in detail, considering both the specific broadband needs supporting them and other key points that emerged in the discussion (but not associated with specific S&T-related needs).

Table 1. Top Needs (Tier 1) from the Broadband Communications Workshop

Problem	Need
Guidance on Managing Future Broadband Networks	
Problem: Law enforcement is likely going to be using hybrid networks combining commercial and FirstNet and existing infrastructure	Need to provide agencies with guidance on how to acquire, manage, and use mixtures of communications networks: wired + commercial bandwidth + FirstNet + existing infrastructure.
Problem: Assumption is that FirstNet devices will (1) be able to log on to FirstNet domain using a set of communications and security standards (LTE -> 5G, Band 14, etc.), and (2) auto-populate with available services and data for that area/jurisdiction/mission at start-up—but what that means operationally is largely to be determined.	Need to develop concepts, policy, and procedures for mutual aid networks in a post land-mobile-radio/FirstNet/broadband era. Need to define the common roles, responsibilities, associated services, information needs, and log-on (authentication and granted permission) capabilities.
Problem: In general, what should the public safety network look like in the future? How should information in general be provided, to whom, and for what purposes? What apps/functionalities do we want to put on officers' devices?	Need to coordinate and integrate operational architecture components being developed (who needs what information, with what attributes) by a number of groups (National Public Safety Telecommunications Council, FirstNet, Global, etc.). Can be built as a layered model with core services (e.g., voice over Internet) to provide with others that can be tailored/deprioritized as needed. Part of this will be conducting an assessment of what data-using functions are most promising to put on devices and what core FirstNet/other services should be available by default. Need to include concepts, policy, and procedures for mutual aid networks. Must explicitly consider data management, legal, and privacy concerns.
Problem: Scale of data being collected/exchanged expected to increase dramatically.	Need to look at how data center/cloud models would work in future network topologies and when, in principle, data centers will need to handle huge amounts of data and may have scalability issues.
Identity, Credentialing, and Access Management	
Problem: Interoperability of communications systems today still requires a lot of prework—very different from the computer world, where third parties can authenticate any device. Need for devices that can connect to many things.	Need new models for general authentication of devices onto a network, more like the Domain Name System (DNS) in computing. Design devices with multiple input/output options, need intelligence in the network (FirstNet as "router") that finds the resource that the device needs to do what it wants to do (one element of 5G is a requirement to allow any device to connect to any network that it is not forbidden to connect with at any time, and there are devices now that default to open WiFi for carrying calls).
Problem: User authentication on new devices becomes more important as the network delivers more access and capability.	Need better ways to do user authentication—make it easy for individual users, such that, for example, if a public safety officer leaves their device behind it is locked, but also accessible by individuals from other agencies.
Problem: There are three identities—the device, the person holding it, and the agency that stands behind it—need a way to do that. Currently, no one is directly taking on that problem.	Need to solve the federated identity management problem to allow authentication of one public safety person with a device to connect to a different network—navigating the challenges posed by local control. Requires a governance model that can make these decisions and take on the education task of getting the message out to the individual departments. Need to develop an equivalent of a certificate authority for authentication for public safety communications—FirstNet will have to solve this problem eventually (i.e., you should be able to use your FirstNet device at a major incident in another state).
Prioritizing Information	
Problem: Officers in the field need more-relevant information pushed to them, while minimizing information overload.	Need research on smart software agents for officers in the field to help them get information they need while avoiding information overload.
Problem: PSAP personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.).	Need to develop processes (including training/staffing), automation filtering and tools, and procedures to help PSAP employees prioritize incoming data and use data to support operations/avoid information overload.

Table 1—Continued

Problem	Need
Problem: PSAP and operations center personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.). What if 10 different people send in video of the same shooting? How can the center manage those streams to use them effectively?	Need to develop core algorithms that can filter and prioritize core types of data coming into PSAPs and operations centers and provide useful products to the field. Need to explore leveraging analytics from the carriers to identify incidents of high interest. Would involve creating archives of PSAP data/footage that can be used by researchers to train algorithms. One is for immediate real-time data and one is for reference information that police might find useful later.
Communications Infrastructure	
Problem: UASs working as communications devices (communications relays), especially as power-tethered UASs.	Need to explore the use of tethered UASs to support rural communications and other areas that need additional communications.
Network Management	
Problem: Law enforcement is likely going to be using hybrid networks combining commercial and FirstNet and existing infrastructure.	Need research on tools and methods on managing hybrid networks that include wired, commercial broadband, FirstNet, and existing infrastructure components.
Problem: Need to decide on priorities for spectrum and specific communications. Need to describe policies for dynamically preempting/getting bandwidth. Current cell downlink maximum for Band 14 is around 7.5 Mbit/sec.	Need to leverage FirstNet work on prioritization and spectrum management to develop a common set of policies and enabling mechanisms for prioritization and spectrum management.
Problem: There are growing opportunities to use best available path algorithms, whether over a "broadband network" or to access an IP point of presence directly.	Need to explore use of dynamic routing mechanisms and tools that will allow devices to pick best available connection points and routes, accounting for user needs, available links, and spectrum and capacity availability.
Problem: PSAP personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.).	Need to explore load-balancing/cross-agency models for PSAPs and operations centers that provide for maintenance of local knowledge and quality, tailored services.
Personnel Development	
Problem: Huge demands on both physical storage and human management of data, including redaction of bystanders/victims in video (currently a manual process).	Need to develop roles for people who specialize in data management of video and other high-volume law enforcement data.
Problem: Communications is migrating toward services architectures rather than dedicated networks. Setup and maintenance activities are changing.	Need to explore what new "communications services" staff or revised training for existing information technology (IT) staff will be needed to address future communications architectures. Need to develop new role descriptions and duties, staffing and training concepts for future PSAP/operations center operations.
Technical Research and Development	
Problem: Antennas are consistently an afterthought.	Need antenna research to extend battery life, reduce interference, improve spectrum efficiency, improve throughput, and reduce size/improve form factors. Technologies include physical design, self-tuning, integration into wearables/other form factors. Also need to consider smart controllers for antennas (part of smart radios).
Problem: Huge demands on both physical storage and human management of data, including redaction of bystanders/victims in video (currently a manual process).	Need better analytics that automate much of the redaction work.

NOTE: There were no Tier 1 needs in the "Policy" area.

Future Information and Communications Capabilities

Coverage and capacity. Coverage repeatedly surfaced as perhaps the most critical need, with one participant stating "coverage is a bigger issue than anything . . . without coverage and capacity, none of the next steps (e.g., what the officer can send or receive) matter—this is an operational need." The terms *coverage* and *capacity* were sometimes used interchangeably, encompassing both access to broadband in areas that are currently not served (rural, etc.) and access in congested areas (e.g., Beach Week, Super Bowl). Coverage and capacity are needed during both emergency and special events and daily operations. Several participants noted that capacity issues occur not only during incidents that are universally viewed as special circumstances or emergencies (e.g., Boston Marathon bombing) but also during times that would traditionally be considered normal daily operations (e.g., high-volume days at the beach). Law enforcement needs preferential access in both circumstances.

Near-real-time tracking of law enforcement persons and vehicles (also known as "Blue Force Tracking") is a clear goal/need for law enforcement, implying the need for continuous relay of data to and from the field. Officer position and location are important, but participants indicated that it is only the base/starting point. Law enforcement also needs officer status information, including "human telemetry," such as indicators of stress/health.

An "Internet of public safety things" may arise that officers and operations centers will receive data from routinely. Participants agreed that 15 years from now there could be a range of new sensors in the field not currently conceived of. Communication needs in the field could go beyond person-to-person; for example, a building may know it has been broken into and notify a PSAP; thermostats inside a building might be able to pinpoint the locations of fires.

Large and highly uncertain data volumes. There are concepts emerging that will require unprecedented volumes of bandwidth. For example, it was noted that, in 10 to 15 years, there could potentially be a million cameras in a typical major U.S. city, plus tens of millions of other sensors that could inform that city's public safety agencies.

Challenge of addressing diversity of agencies. The diversity of the law enforcement/public safety community emerged as an underestimated and critical factor. It was noted that there are approximately 6,000 PSAPs (National Emergency Number Association, 2015), 18,000 law enforcement agencies (Reaves, 2011), and 60,000 total public safety/first responder agencies (First Responder Network Authority, 2015b), all with their own purchasing processes, procedures, etc. There is not a unified or uniform public safety/law enforcement community, and this will increase the difficulty of managing the future of public safety broadband.

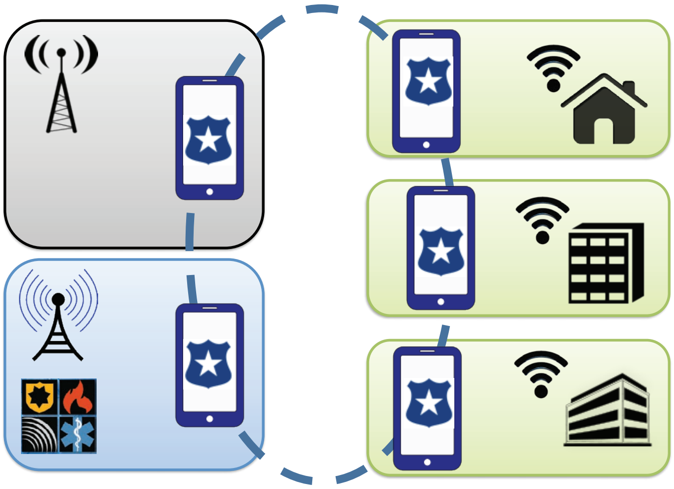
Enabling the Future Network

The first theme is supporting the emergence of a future broadband network in which law enforcement users will be able to seamlessly and securely communicate over whatever local point of access is the best fit at any specific location, time, and situation. As shown in Figure 3, a future device might communicate over commercial 4/5G stations, FirstNet stations, other government-owned 4/5G stations, commercial Internet wireless access points, and even private wireless access points that permit secured sharing. This will be an expansion and automation over smartphones' and tablets' current capabilities to hop between 4G carrier service and wireless Internet access points that the devices have been manually configured to access.

Network management in this future environment will cease to be about managing specific sets of equipment (or bandwidth usage permitted under a specific 4G commercial contract) and instead become virtualized. Future network management will involve dynamically reallocating different types of connections, spectrum being used, and other types of bandwidth to meet changing force deployments and operational needs.

Participants discussed many early examples of this evolution. They noted that commercial networks are already develop-

Figure 3: The Future Broadband Network: One Device, Many Types of Connections



RAND *RR1462-3*

ing to become heterogeneous networks ("het nets") in urban areas. Looking 10 to 15 years out, several participants described visions of this heterogeneous environment. Accordingly, the challenge will be "how to make sure the law enforcement device finds the best available spectrum access for the application's unique needs." It was noted that some major commercial companies are doing research in this area now, but it needs to be done "on steroids."

From the federal perspective, FirstNet representatives indicated that it would be beneficial to genericize the discussion to broadband—FirstNet will build a network, but all public safety may not subscribe to it. The discussion should not be "FirstNet should do this" but should be "the heterogeneous network should do this." FirstNet representatives also noted that the current concepts were to combine FirstNet with commercial networks.

The heterogeneous network was also seen as extending to the personal level of officers and their vehicles. In the future, participants described how the officers or vehicles may themselves be the "hot spots." An officer/deputy's personal devices would sync up with the car when he or she arrives, with potentially just a "dumb two-way screen" in the car. Apps could be on the officer's phone; mirror-casting could be utilized. One participant noted that at least three commercial companies are working on this now. Another participant asked whether this was thinking too short-term—"Will it not be smartphones/tablets at all, but wearables?" Another participant noted that rural officers are usually with their vehicles, so it makes sense to harden the vehicle, and make it the hot spot.

A majority of Tier 1 needs cover different aspects of this future network, including defining what it will be, developing guidance for agencies, and conducting technical R&D on future devices and management tools.

Envisioning the Future Network. Perhaps the most fundamental needs were to have multiple stakeholder organizations develop operational concepts and architectures to define what the future network should look like and how it should work to best support law enforcement requirements. Common types of services (push-to-talk voice over Internet, maps, etc.); data flows responders need on a day-to-day basis; and their sources, qualities, and attributes need to be identified. There was also a call to look beyond communications links to examine how data center and cloud models might handle the huge amounts of data expected to come off of broadband networks. Several participants noted that FirstNet, the Department of Homeland Security's interoperability initiative SAFECOM, and others are working on this now, although efforts were described as "scattered."

Envisioning the Role of FirstNet. A key element (but only one element) here is to provide more detail on what FirstNet will and will not provide, and how. While not directly generating many needs, discussions and debates about FirstNet took up more of the panel's time than any other single topic. That said, the distinction between FirstNet and broadband in general was frequently blurred. Although the session was clearly cast as "broadband communications opportunities and problems," participants seemed to have difficulty maintaining the distinction between broadband in general and the specific FirstNet network. Ultimately, there was acknowledgement that "FirstNet can't do everything—its job is to build a pipe." The Tier 1 needs for developing clear concepts and architectures about the future network were in part drawn from confusion about what exactly FirstNet will provide and when, how it will work, and how the FirstNet business model will work, versus what commercial firms and agencies themselves will be expected to provide.

Participants noted that two overall goals for FirstNet are coverage where commercial coverage doesn't exist (rural, etc.) and reliable coverage at all times—e.g., coverage during congestion. Security and resilience are the two main reasons the law enforcement community would prefer not to use a commercial network. Carriers have legal reasons for not wanting to kick private customers off for public safety users (liability); however, participants suggested that some of this is just a negotiating tactic. Market issues also dominate many commercial coverage decisions: One participant noted that "there are FCC [Federal Communications Commission] licenses that sit barren and unused in rural areas because there is no market." One participant noted that "there is a need for public-private partnerships,

> Security and resilience are the two main reasons the law enforcement community would prefer not to use a commercial network.

because I don't expect more money or more spectrum. Congestion is a management issue. We will manage public safety spectrum differently than the commercial sector does—that's why we wanted our own spectrum. All paying customers are the same to the commercial carriers."

Managing the Data Flood. Data storage and archiving will be a huge technical, legal, and policy issue. Participants noted that there is a sense that all of the footage being generated from new body cameras "probably has to go into evidentiary archive" and that the volume, which is truly massive, will only grow. Going forward, there will be additional human telemetry data. Further, advancements could come to service weapons—e.g., cameras mounted on the service weapon. A participant noted "Everything we are talking about generates data, which some lawyer will demand, so it needs to be stored." Even if data are not stored, the potential demands from streaming are massive and need to be considered in future network architectures. One participant noted, "We cannot stream all of this, [so we need to identify] what do we need in order to locate and authenticate?" Similar comments included, "Just because you have a million surveillance cameras, does not mean you can or even should stream all of them at any one time."

Guidance for Law Enforcement Agencies. Other Tier 1 needs further specify the types of guidance agencies will need to acquire and operate virtual networks within the larger future broadband communications architectures. These include providing relevant policies, procedures, and acquisition guidance. Beyond individual agencies, there were similar calls to develop policies, procedures, and acquisition guidance for state and regional mutual aid networks (as part of a larger call for architectural development). The Tier 1 need specifically calling for providing agencies with guidance on "how to acquire, manage, and use mixtures of communications networks" was the top-rated need of the workshop.

Technical Requirements for Future Devices. Several Tier 1 needs cover technical requirements for devices to be part of the hybrid network. These include R&D for device antennas to extend range and service quality; R&D for devices to connect to different types of PSAPs and smartly choose between them; R&D for seamlessly getting and maintaining authentication as devices hop between Internet access points; and R&D for ensuring secure transmission of sensitive law enforcement information across multiple types of PSAPs, including private and commercial.

Spotlight: Antenna Research. One participant felt strongly, and was supported by others (including through a Tier 1 need), that additional attention needs to be paid to antenna technology, which is currently "consistently an afterthought." Improving antenna technology so that antennas could radiate only in the (one) direction of interest would improve battery life, data throughput, and capacity/efficiency. The need is for smart antennas with smart control; initially they will need to be vehicle-mounted due to size. That said, other panelists opposed this area of research on grounds that it was unlikely that small law enforcement–focused projects would improve on huge commercial investments in antenna development.

Data storage and archiving will be a huge technical, legal, and policy issue.

A Larger Debate: Commercial vs. Customized Devices. While not R&D needs per se, there was a good bit of discussion on whether the law enforcement community should seek to use commercial devices, even if they have operational shortfalls, or custom-made devices, even if they take longer to develop and are more expensive. Several participants noted that developing devices uniquely for public safety is "slowing things down." Some police departments have found it better to live with the deficiencies of commercial devices because they are cheaper, do more, and are available now. One participant noted that it "is cheaper to buy commercial, it breaks in a year, and buy a new one every year, than to buy a ruggedized more expensive public safety device." One participant noted that designing mission-critical handheld devices (e.g., which can "withstand a 6 foot drop") is not a hard engineering challenge, there is just no economic incentive right now. There was discussion that law enforcement is on a precipice between going with commercial devices and "going the route of the $5,000 land mobile radio (LMR)" with its future field-use broadband devices. One participant noted "there is no middle path" between using commercial-based government-owned devices and public safety–specific devices and that a "fundamental decision needs to be made about whether to leverage commercial and live with its limitations or go for our own specialized devices but risk winding up with $5,000 radios like we did with LMR."

Another variant of this decision is utilizing ruggedized devices or officers' own devices ("bring your own device"). Participants noted the problem of personal devices in the field: Officers today are using their personal phones to take photos and videos while on duty, which are then seized as evidence or subject to Freedom of Information Act (FOIA) requests. The New York Police Department and a number of other agencies have issued policies that officers may not use personal phones for video, etc., because of evidentiary and FOIA concerns. However, another participant noted that bring-your-own-device is an important idea. It would require derived credentials; officers could use their device in a sleeve—"this would be an elegant short- to mid-term way to get a very large number of devices on FirstNet, and bringing a large number of devices onto FirstNet is critical to FirstNet succeeding."

Network Management Tools. Outside the device, Tier 1 needs call for the development of the network management tools that will be needed to dynamically configure and maintain the future hybrid network. These specifically include tools that can dynamically adjust data priorities and spectrum allocations to meet changing user needs.

High-level Network Management Issues. Participants noted that while long-range forecasting of demand is important, and there may be some relevant cases to study today, demand will always come down to a management issue. One participant suggested that demand will "always be a little greater than capacity because that's how things work." The ability to prioritize and manage spectrum is an operational need; so is the need to access alternative spectrum—datacasting, white space. Discussions need to be had about how to use alternate spectrum resources, such as white space, when public safety needs it. This would require FCC approval, but many participants envisioned scenarios in which public safety would use white space during certain emergency conditions. Examples currently exist in which law enforcement is using bandwidth inappropriately—e.g., "the midnight shift streaming video and using up bandwidth"; there may be a need for an intranet (vs. Internet) and "firewalls with select holes."

A Requirement for Management: Usage Metrics. Metrics need to be developed for bandwidth utilization and other aspects of public safety broadband utilization. There was agreement that opportunities currently exist, but are not being leveraged sufficiently, to determine current levels of utilization and what they may look like in the future. FirstNet representatives stated that FirstNet is asking each state, as part of the request for proposal (RFP) process, to describe how it is using data today and how the state intends to develop "some sort of national picture" on how public safety data will need to be used in the future. Carriers currently have a wealth of usage data, but panelists noted that these data have not been mined for this purpose. Another participant noted that the recent rise in body cameras represents a major shift that will begin to develop a public safety utilization picture; however, patterns are also likely to vary between urban and rural police departments, police and fire, etc., rather than being homogeneous.

Extension to Rural Areas. There was also a need to ensure that the hybrid network extends to rural areas. Panelists repeatedly noted that it is critical that rural areas be provided with the full broadband coverage and capacity needed to support law enforcement operations. Broadband is not just for densely populated areas.

The top-rated need in this area called for *experimenting with tethered UASs* to provide coverage. This need was prioritized third overall. Tethered UASs emerged as a popular idea for solving some rural, and even urban, coverage issues. A tethered UAS provides the prospect of "a 100-foot antenna that can go up in 60 seconds." With power provided via the tether, the UAS can serve as a communications platform and can provide coverage in rural areas, or at a minimum a zone of coverage for the area under it for the officer; another participant noted there are urban applications for this technology as well. Additional communications may be needed due to congestion, etc.

Security. How security will work in the new network environment in general was a major topic of discussion at the conference. As might be expected, security and authentication emerged as big issues for law enforcement. Discussion was sometimes not specific or conversely focused on a single example (hacking leading to release of the Ferguson dispatch tapes; existing cell phone jammers), but there was general agreement that security and authentication were critical needs.

> How security will work in the new network environment in general was a major topic of discussion at the conference.

As articulated by one participant, there is a "need for positive control—we need to know who is on the network." Similarly, participants agreed that while authentication is needed, it needs to be agile and available during emergency situations requiring the arrival of mutual aid from out of state and from various levels of government or unexpected (but validated) partners. There was discussion of potential current models, such as university wireless network reciprocity agreements or systems. Several Tier 1 needs concerned building in authentication and information protection as devices hop around the new heterogeneous broadband networks.

Standards. Participants agreed that there is a need for standards, but that developing standards is difficult and time-consuming. Participants agreed that standards and standardization are a major issue, but one participant cautioned that setting standards can take a prohibitive amount of time and that often halfway "community consensus" approaches could be sufficient.

Policy. While not generating Tier 1 needs, the group did agree that there are many law, policy, practice, disciplinary, and privacy issues that must be resolved when envisioning how law enforcement will leverage future heterogeneous networks. As just a few examples, in one jurisdiction officers had to be reminded to turn off body cameras when going to the bathroom. In another jurisdiction, in an officer-involved shooting, the officer claimed the camera stopped working and was fired when the provided data indicated this was impossible.

Making Sense of Information in the New Network

The second major theme that emerged from the workshop is users being able to filter, prioritize, and make sense out of all the new data scheduled to be shipped over the new broadband network. A common concern was the danger of information or data overload and how to manage and curate information to make it most useful for various levels of law enforcement (PSAPs, officers in the field, etc.). There is a danger of the volume of incoming data and information vastly exceeding the ability of the law enforcement community to manage it—for example, every person driving by a crash sending a picture to the PSAP. Needs in response covered both technical R&D and development and training of new information-centric roles.

For the field, there was a top-ranking need to develop *smart software agents* that could accurately display what an officer needs to best do his or her job in a given situation while reducing information overload. Here, a smart software agent is a software program that can search for, select, and customize a display of information to a user automatically, using a combination of manually set inputs and machine learning to assess what the user should consider to be most important. (For a technical treatment, see Russell and Norvig [2009].) This need was rated as the second-highest priority overall. Information to officers in the field should be "filtered down to what they need to make a decision." Participants noted it was unclear where automated analysis to filter and prioritize information would reside (PSAP level, officer level, combinations, etc.). More broadly, it was noted that officers need simplicity. The number of devices or methods to accomplish tasks must be limited. On scene, officers are already carrying large amounts of equipment on their person. In the vehicle, participants noted that digital distractions are already a huge issue for officers, and technologies and smart software agents that can address this would help make the vehicle a safer place.

For operations centers, there were top-ranking calls for new smart software agents to help PSAP telecommunicators better prioritize an anticipated flood of new types of information coming with 911 calls for service and sensor alerts (photos and video, notably). Participants said that an algorithm (for example) was needed to weed out what information, photos, and data are not useful, are repetitive, etc., on grounds that call-takers at a PSAP cannot do this, nor should they have to. Several participants noted that Google image search and other currently available software can do this, with PSAPs able to leverage existing tools—"this is not a DARPA [Defense Advanced Research Projects Agency] problem." One participant suggested there is a need to reverse engineer the capability for law enforcement by taking an incident and everything that comes in, figuring out what would have been useful to know as it came in, and building an algorithm that pulls that content out. It was also noted that news media are very good at reviewing enormous amounts of film footage quickly, grabbing what they need and using it, and perhaps what they do can be learned, used, and automated for law enforcement.

There were specific calls for *tools that will help manage the anticipated flood of video footage*; there is an especially acute need for a tool that can automatically redact the faces and voices of bystanders (currently a manual process). The time needed to process video for FOIA requests is substantial, even prohibitive. A participant noted that it is estimated that one agency (Dallas) needs 17 labor hours to release a short clip requested via FOIA or discovery. The time-consuming component is going through the media to redact identifiers—while the technical redaction process is not complicated, the need to apply judgment and determine what needs to be redacted is (faces, minors, victims, addresses, etc.).

At a higher level, there was a call for *developing load balancing tools and concepts* that would help allocate people and equipment more efficiently at PSAPs and operations centers. These explicitly included developing cross-agency load-sharing models that would permit, for example, timely answering of routine 911 calls for service during a major incident that overwhelms a single PSAP by another PSAP. Some participants noted this may require a culture shift as well as a governance shift. Panelists had concerns that cross-agency or cross-jurisdictional efforts would be difficult and perhaps unlikely: "The governance question is huge—you can throw tech at it all day, but you need the police chief and sheriff to work together."

For training and development, there were top-ranking needs to develop and train on new types of roles that will be needed to manage and exploit the new data flows. These included roles for PSAP data management and video management specifically. Participants noted that PSAPs will need to change training and maybe even job duties for call-takers. There was discussion over whether there would be a need to "hire someone just to look at and edit video." Participants noted that PSAPs are already overwhelmed and understaffed. In the future, participants anticipated that the job may look more like an air traffic controller, and will need to be better paid.

Relevance for Incident Command. The difficulties managing information experienced in future PSAPs will (and already have) hit incident command posts as well. Participants said that information management and technical communications are getting so complex that there is a need for a communications position, with specialized training, on the incident command system chart. One participant noted that IT support is now needed to accompany the communications person. Another noted that these are exactly the types of operational needs that should be identified for law enforcement: "Part of the service economy is when you get on a network, it downloads its personality. Comm L [Communications Leader] stuff should be automatically downloaded (e.g., who is on site, contact information, etc.), even if you are from a different agency or jurisdiction."

CONCLUSIONS: SETTING THE TECHNOLOGY AGENDA

To conclude, we present ways to take action on the themes and specific needs, providing a S&T roadmap for broadband-related development for law enforcement.

Developing the core architecture for the future hybrid network. The central recommendation is to develop a core set of operational concepts and architectures that will lay out, as clearly as possible, what the future hybrid network will look like for law enforcement (and other public safety) agencies, how agencies will access it, and what services it will deliver. We envision the Public Safety Communications Research (PSCR) laboratories and FirstNet leading what will primarily be a coordination and integration activity, similar to what the new Standards Coordinating Council is attempting with the wide range of data-sharing standards (Standards Coordinating Council, 2015). Thus, the effort needs to begin first by identifying a suitable sponsor for the work that can bring together the multiple key operational and technical stakeholders. The next step will be identifying needed architectural views, concepts, and standards, including what largely exists and just needs to be complied with and what needs to be built. Similarly, there is a need to identify common policies and memoranda of understanding to support these elements. Perhaps the most important upfront task will be to identify which agency should be in the leading role along with other agencies in supporting roles; as noted, existing conceptual and architectural work is scattered.

> The central recommendation is to develop a core set of operational concepts and architectures that will lay out, as clearly as possible, what the future hybrid network will look like for law enforcement.

The architectures' use cases should include those specified in Tier 1 needs, including general routine and emergency or major incident case handling, "blue force tracking" telemetry (location, status, health monitoring, other situational monitoring), video camera integration, Internet of Things sensor integration, and data center/cloud structures for storing and managing the incoming data. Some sense of reasonable subnet structuring and scheduling, filtering, and monitoring should be built in to network architectures. Similarly, network applications and users need to be sensitive to the latency impacts of high-bandwidth data transfers so that the future network will not be swamped with, say, a million cameras attempting to transmit high-definition feeds at once. On the opposite end, the architectural products will need to identify how rural and/or sparsely populated areas will receive reliable broadband coverage. An additional key piece will be to clearly specify what capabilities FirstNet will deliver, to whom, and when.

Given that the core attribute of the future network is that devices are to hop seamlessly across different Internet points of presence with different governance (e.g., FirstNet via commercial) and even different waveforms (e.g., short-distance 802.11x vs. 4G vs. 5G), much of the architectural effort needs to address how such hopping will work.

The next core attribute of the future network is security. Much of the architectural efforts will need to cover a range of security issues, including identity, credentialing, and access management (ICAM) for the new networks; ensuring end-to-end security of transferred data (encryption, etc.); and the mechanics of how a device will request and gain permission to transmit data across third-party Internet points of presence in ways that will ensure that the privacy and integrity of both the law enforcement data and other data on that point of presence is protected.

Guidance for agencies. The top-rated need of the workshop had to do with providing agencies with guidance on how to acquire, manage, and use the forthcoming hybrid networking technologies. Directly dependent on the architectural work above, one set of guidance materials should provide individual agencies with plain-English use cases and other architectural material, policies, procedures, and acquisition guidance. The second set should be similar in nature but apply to state and regional mutual-aid networks. Note that these deliverables depend on at least partial maturation of the conceptual and architectural products described above. We envision the Department of Justice sponsoring the development of guidance for law enforcement agencies.

> The top-rated need of the workshop had to do with providing agencies with guidance on how to acquire, manage, and use the forthcoming hybrid networking technologies.

Technical assessment studies. There were a range of top-rated needs that called for technical improvements to devices. These were somewhat controversial, as some panelists noted that (1) any small amounts of R&D funding NIJ and other Office of Justice Programs funders could provide would be dwarfed by commercial telecommunications investments and (2) in general, the law enforcement broadband market is much too small for the field to make special requirements on its devices, unless it wants to pay a very high price per device. Our suggested solution is for the Department of Justice to sponsor technical assessment studies examining whether it is possible to make better use of existing technologies in both the general commercial and ruggedized commercial markets for law enforcement broadband. The lead organization for each assessment would be responsible for doing the study and preparing products that disseminate the results to both practitioners and technology developers. Assuming that it is feasible to field modified devices that better meet law enforcement's needs at reasonable prices, the next step would be development efforts, with some likely funded by federal agencies and others funded directly by industry, depending on the specifics.

As noted in the table of needs, specific assessments called for include antennas (improving range, effective throughput, and human factors/shape); devices capable of service-hopping, including picking which available service would provide best performance; and devices that can maintain seamless security (authentication and information assurance) across service hops.

There was also a call to assess what would need to be done to make standard commercial devices suitable to be used with FirstNet and other secure law enforcement networks, as this will be needed to permit the use of bring-your-own-device on future law enforcement networks. One concept was to develop some sort of smart sleeve that would plug into commercial devices and access secure law enforcement devices.

Outside of devices, there was a highly rated call for a technical assessment of using airborne UASs to serve as communications relays.

Sense-making. As with the technology assessments for devices, we recommend that the Department of Justice sponsor technology assessments of what smart software agent technologies are currently available and could be adapted for law enforcement rather than starting with all-new R&D. For this theme, there was one top-rated need for smart software agents that can prioritize what officers in the field need to see in different operational contexts and reduce information overload.

More of the sense-making needs applied at the operational level, for PSAPs and operations centers in particular. These included smart software agents to prioritize incoming data, with one call for agents that could analyze data submitted as part of calls for service and one call for agents that could filter and prioritize torrents of data coming from video and Internet of Things sensors.

Also of very high interest were tools that could automate redaction of video feeds. Again, this should be a technical assessment, as commercial tools to do this are emerging.

Outside of technology, also of high interest were needs for new job descriptions and corresponding training materials for emerging PSAP and operations center jobs for working with the forthcoming flood of photos, video, and Internet of Things data.

Summary. Finally, Table 2 provides a summary of the major issues, recommended ways ahead, and associated key milestones. All are intended to provide maximum expected value to the practitioner in bringing increased communications capabilities to law enforcement.

Table 2. Summary of Broadband Issues, Recommendations, and Associated Milestones

Issue	Recommendations	Milestones
Future Architectures		
Concepts and architectures for future hybrid broadband networks are insufficient	Develop concepts and architectures for the future hybrid networks, including • Identify leads and supporting roles • Integrate existing products • Include key operational use cases • Describe coverage for rural areas • Explain service-hopping • Build in security and authentication provisions • Build in filtering and scheduling	• Sponsor, lead, and supporting roles for integration and development identified • Base concepts and cases completed • FirstNet capabilities specified • Advanced concepts and architectural products completed
Guidance for Practitioners		
Practitioners need guidance for emerging broadband technologies	• Develop guidance on future broadband technology acquisition, management, and use for individual agencies • Develop guidance for state and regional mutual aid networks	• At least base concepts and cases from above completed • Guidance for agencies prepared • Guidance for mutual aid networks prepared
Technology Assessments		
Need to assess whether technologies can improve the functioning of devices used for law enforcement	Conduct technical assessment studies of device • Antennas (range, throughput, shape) • Service-hopping capabilities • Best pick of service capabilities • Authentication across service hops • Information assurance across service hops	(For all technology assessments) • Lead for assessment study identified • Study completed • Results disseminated to both practitioners and technologists • Follow-on development efforts (if appropriate) started • Technical assessment studies for device technologies completed
Need to assess suitability of bring-your-own-device for future law enforcement networks	Conduct a technical assessment of using commercial devices for future law enforcement networks, and assess ways to improve suitability (including developing a plug-in sleeve for accessing secure networks)	
Need to examine the use of UASs as relays	Conduct a pilot study of the use of UASs as communications relays for law enforcement network	
Sense-Making		
Need to assess smart software agents for the field	Conduct a technical assessment of technologies that can prioritize displays and reduce information overload across different operational contexts	(Same as for technology assessments)
Need to assess smart software agents for the operations center	Conduct technical assessments of agents that offer promise to be able to • Prioritize data from calls for service • Prioritize data from routine monitoring and sensor feeds (video, other)	
Need to redact video feeds automatically	Conduct technical assessments of emerging products that automate video redaction	
Need to develop emerging operations center roles	Develop descriptions and concepts for new operations center roles that involve working with large quantities of incoming data Develop training material for the new operations center roles	• Descriptions and concepts completed • First iteration of training material completed

Members of the Broadband Communications Panel

Ahsan Baig, City of Oakland, Information Technology Department
Vanu Bose, Vanu Inc.
Milind Buddhikot, Alcatel-Lucent Bell Labs
Jack Burbank, Johns Hopkins University Applied Physics Laboratory
Jeremy Carter, Indiana University—Purdue University Indianapolis (IUPUI)
Stanley Causey, Department of Justice, Drug Enforcement Administration
Bedri Cetiner, Utah State University
R. (Mouli) Chandramouli, Stevens Institute of Technology
Hao Chen, University of California at Davis
Randy Clark, Oceus Networks
Daniel Devasirvatham, Department of Energy, Idaho National Laboratory
Josh Ederheimer, FirstNet
Scott Edson, Los Angeles Sheriff's Department
Ahmed Eltawil, University of California at Irvine
Joel Estes, Adams County Communication Center (ADCOM911)
Laurie Flaherty, National Highway Traffic Safety Administration, Office of Emergency Medical Services
Franklin Flint, Telecommunications Industry Association
Fred Frantz, Engility
Declan James Ganley, Rivada Networks
Phil Harris, Engility
Brian Kassa, FirstNet
James Ketsaa, Clark County (Nevada) School District Police Department
Joe Kochan, US Ignite
Jonathan Lewin, Chicago Police Department and Office of Emergency Management and Communications
Shing Lin, Harris County (Texas) Information Technology Center
Preston Marshall, Google, Inc.
Harlin McEwen, International Association of Chiefs of Police
Thyaga Nandagopal, National Science Foundation
Stagg Newman, Qualcomm
Mark O'Brien, SpectraRep
Parmesh Ramanathan, University of Wisconsin–Madison
Eddie Reyes, Alexandria Police Department
Allan Sadowski, North Carolina FirstNet Single Point of Content (SPOC)
Brian Shepherd, Colorado FirstNet SPOC
Darrel Stephens, Major Cities Chiefs
Rangam Subramanian, National Telecommunications and Information Administration
Scott Valcourt, University of New Hampshire
Joseph Wassel, U.S. Department of Defense FirstNet
Jack Weiss, BlueLine Grid
Kevin Wennekes, CATAAlliance (Canadian Advanced Technology Alliance)
Karen Wong, California FirstNet SPOC

References

Akyildiz, Ian F., Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey," *Computer Networks*, Vol. 50, No. 13, 2006, pp. 2127–2159.

Akyildiz, Ian F., Josep Miquel Jornet, and Chong Han, "Terahertz Band: Next Frontier for Wireless Communications," *Physical Communication*, Vol. 12, September 2014, pp. 16–32. As of August 9, 2016: http://www.sciencedirect.com/science/journal/18744907/12/supp/C

Chan, Vincent W. S., "Free-Space Optical Communications," *Journal of Lightwave Technology*, Vol. 24, No. 12, 2006, pp. 4750–4762.

Chandrasekhar, Vikram, Jeffrey G. Andrews, and Alan Gatherer, "Femtocell Networks: A Survey," *IEEE Communications Magazine*, Vol. 46, No. 9, 2008, pp. 59–67.

Federal Communications Commission, "White Space Database Administration," *FCC Encyclopedia*, November 10, 2015. As of August 9, 2016:
https://www.fcc.gov/encyclopedia/white-space-database-administration-q-page

———, "700 MHz Public Safety Spectrum," 2016. As of August 9, 2016:
https://www.fcc.gov/general/700-mhz-public-safety-spectrum-0

First Responder Network Authority, "FirstNet Industry Day," presentation to the FirstNet Industry Day, Reston, Va., August 27, 2015a. As of August 9, 2016:
http://www.firstnet.gov/sites/default/files/Aug%2027%20Industry%20Day%20Presentation_2.pdf

———, "FirstNet by the Numbers," FirstNet.gov, September 2015b. As of August 9, 2016:
http://www.firstnet.gov/sites/default/files/FNBTN_151019_v2.pdf

Goodison, Sean E., Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, Santa Monica, Calif.: RAND Corporation RR-890-NIJ, 2015. As of August 9, 2016:
http://www.rand.org/pubs/research_reports/RR890.html

Hollywood, John S., John E. Boon, Jr., Richard Silberglitt, Brian G. Chow, and Brian A. Jackson, *High-Priority Information Technology Needs for Law Enforcement*, Santa Monica, Calif.: RAND Corporation RR-737-NIJ, 2015a. As of August 9, 2016:
http://www.rand.org/pubs/research_reports/RR737.html

Hollywood, John S., Dulani Woods, Richard Silberglitt, and Brian A. Jackson, *Using Future Internet Technologies to Strengthen Criminal Justice*, Santa Monica, Calif.: RAND Corporation, RR-928-NIJ, 2015b. As of August 9, 2016:
http://www.rand.org/pubs/research_reports/RR928.html

Hollywood, John S., and Zev Winkelman, *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?* Santa Monica, Calif.: RAND Corporation, RR-645-NIJ, 2015. As of August 9, 2016:
http://www.rand.org/pubs/research_reports/RR645.html

Kennedy, T. J., "First Net Update," presentation to the Association of Public Safety Communications Officials Broadband Summit, Washington, D.C., May 4, 2015.

Minoli, Daniel, *Innovations in Satellite Communication and Satellite Technology*, Hoboken, N.J.: Wiley, 2015. As of August 9, 2016:
http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118984056.html

Monsen, Peter, "Tropospheric Scatter Communication," *Encyclopedia of Telecommunications*, Hoboken, N.J.: Wiley, 2003.

National Emergency Number Association, "9-1-1 Statistics," NENA.org, 2015. As of August 9, 2016:
https://www.nena.org/?page=911Statistics

National Law Enforcement and Corrections Technology Center, "What Is Datacasting, Anyway?" *TechBeat*, Summer 2012. As of November 24, 2015:
https://www.justnet.org/interactivetechbeat/summer_2012/Whatisdatacastinganyway.pdf

Next Generation Mobile Networks Alliance, *NGMN 5G White Paper*, Frankfurt, Germany, February 17, 2015. As of October 5, 2015:
https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

Olewitz, Chloe, "Thanks to an Ultralight Power Tether, This Surveillance Drone Can Stay Aloft Forever," Digital Trends, November 10, 2015. As of November 24, 2015:
http://www.digitaltrends.com/cool-tech/eyes-in-air-perpetual-flight-surveillance-drone-never-lands/

Perkins, Charles E., *Ad Hoc Networking*, Addison-Wesley Professional, 2008. As of November 24, 2015:
http://dl.acm.org/citation.cfm?id=1481270.

Reaves, Brian A., *Census of State and Local Law Enforcement Agencies*, Washington, D.C.: Bureau of Justice Statistics, 2011.

Rinqvist, Patrik, "Public Safety LTE Technology Evolution," presentation to the Association of Public Safety Communications Officials Broadband Summit, Washington, D.C., May 4, 2015.

Russell, Stuart, and Peter Norvig, *Artificial Intelligence: A Modern Approach*, Upper Saddle River, N.J.: Prentice Hall, 2009.

Sezer, Sakir, Sandra Scott-Hayward, Pushpinder Kaur Chouhan, Barbara Fraser, David Lake, Jim Finnegan, Niel Viljoen, Marc Miller, and Navneet Rao, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," *IEEE Communications Magazine*, Vol. 51, No. 7, July 2013, pp. 36–43.

Silberglitt, Richard, Brian G. Chow, John S. Hollywood, Dulani Woods, Mikhail Zaydman, and Brian A. Jackson, *Visions of Law Enforcement Technology in the Period 2024–2034: Report of the Law Enforcement Futuring Workshop*, Santa Monica, Calif.: RAND Corporation, RR-908-NIJ, 2015. As of August 9, 2016:
http://www.rand.org/pubs/research_reports/RR908.html

Standards Coordinating Council, homepage, 2015. As of January 8, 2016:
http://www.standardscoordination.org/

Tozer, T. C., and David Grace, "High-Altitude Platforms for Wireless Communications," *Electronics & Communication Engineering Journal*, Vol. 13, No. 3, June 2001, pp. 127–137.

Acknowledgments

The authors would like to acknowledge the participation and assistance of the panelists of the 2015 Broadband Communications Workshop. We would also like to acknowledge the contributions of Joseph Heaps and William Ford of the National Institute of Justice, as well as the peer reviewers of the report: Sasha Romanosky, Craig Fraser, and two anonymous peer reviewers selected by the National Institute of Justice.

RAND Justice Policy

The research reported here was conducted in the RAND Justice Policy Program, which spans both criminal and civil justice system issues with such topics as public safety, effective policing, police–community relations, drug policy and enforcement, corrections policy, use of technology in law enforcement, tort reform, catastrophe and mass-injury compensation, court resourcing, and insurance regulation. Program research is supported by government agencies, foundations, and the private sector.

This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy- and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the project leader, John S. Hollywood (John_Hollywood@rand.org). For more information about RAND Justice Policy, see www.rand.org/jie/justice-policy or contact the director at justice@rand.org.

About This Report

On behalf of the U.S. Department of Justice's National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum, RTI International, and the University of Denver, is carrying out a research initiative to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise.

In September 2015, RAND conducted an expert workshop on broadband communications technologies for law enforcement. This document reports on the proceedings of that workshop, discussing the technologies considered, the needs that the panel developed, and overarching themes that emerged from the panel's discussions. It should be of interest to NIJ and other government agencies involved in research on technologies for the criminal justice community, private sector technology providers, agencies within the criminal justice community, and those looking at the future of criminal justice and technology more broadly.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND
CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND®** is a registered trademark.

RR-1462-NIJ