ctc technology & energy
engineering & business consulting

Critical Partners in Data Driven Science: Homeland Security and Public Safety

Submitted to the *Workshop on Advanced Regional & State Networks: Envisioning the Future as Critical Partners in Data-Driven Science*

Andrew Afflerbach, Ph.D., P.E.
Director of Engineering and CEO, CTC Technology & Energy
Member, Public Safety Advisory Committee to the FirstNet Board of Directors
Member, SAFECOM Emergency Response Committee

Regional and state networks play significant roles in public safety communications. This collaboration must increase as the needs of public safety and first responders grow and become more data driven; as the collaboration between public safety and university communities increase; and as the cost of critical resources and skilled staff continues to rise.

As an example, to fulfill a critical, time-sensitive need for a network with a demonstrated track record, the National Capital Region (NCR) selected the Mid-Atlantic Crossroads (MAX) GigaPOP to provide a secure high-speed connection between the three states (District of Columbia, Maryland, and Virginia). MAX provided the first interconnection between formerly separated, stove-piped, local government fiber optic networks and made possible the development and deployment of some of the first high-bandwidth, regional public safety applications across a massive region.

The MAX interconnection was activated in 2005 between existing public safety/research peering points at George Washington University, University of Maryland, and an Internet POP operated by Level(3). The initial connection was over dedicated 2.5 Gbps wavelengths, one of the largest pipes then in use for public safety communications. Within weeks of first contact, MAX provided a diversely routed core that continues to sit at the center of the network.

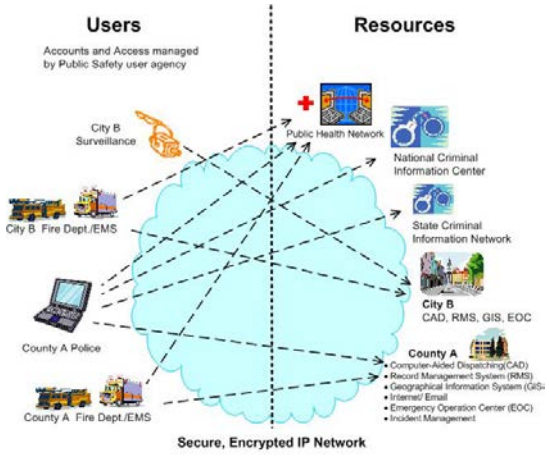

Figure 1: Public safety communications require multiple, survivable paths between users and resources of diverse jurisdictions and agencies.

Public safety needs are extensive and costly. In order to be ready and not simply prepare for a repeat of the last emergency (9/11, Katrina), first responders and emergency managers develop a mesh of redundant practices, devices, and technologies centered around a core of technologies that are well-proven operationally, such as land mobile radio. Now that public safety mobile data applications have been in use for more than a decade, these applications are

now part of that core, and mobile broadband has become a key need in tandem with land mobile radio.

Key metrics for the next generation public safety network are 1) availability in all hazards, all emergencies, 2) guaranteed security/isolation from other networks, 3) scalability to accommodate the transition from voice and text to video, images, and advanced analytics, 4) connectivity between disciplines, regions, and jurisdictions, both to facilitate coordination and to enable joint development and hosting of applications, and 5) capability to receive and process a breadth of data from the public and a wide range of sensors and technologies.

Risks and gaps include 1) few uniform standards exist for public safety grade and resource hardening, 2) needs for more flexible solutions grow as budgets dwindle, and 3) jurisdictions and agencies face challenges to financially sustain existing systems and operations.

Public safety and homeland security networking has grown from simple voice and manual processes to become increasingly data driven. Public safety users face adversaries with sophisticated technology capabilities, and public safety often succeeds or fails on the strength of its network and its devices. First responder applications include multimedia and graphical databases (criminal, hazardous materials), closed circuit video, biometric recognition, WMD detection, geographic (GIS) analytics, and a wide range of GPS-based applications. Incident management involves immediate access and analysis of diverse maps, blueprints, property records, logs, flight lists, and social media materials. Incident managers take information from the public through calls but also social media, text and email. Similarly, public alerting must go through all available media and must also be capable of niche targeting.

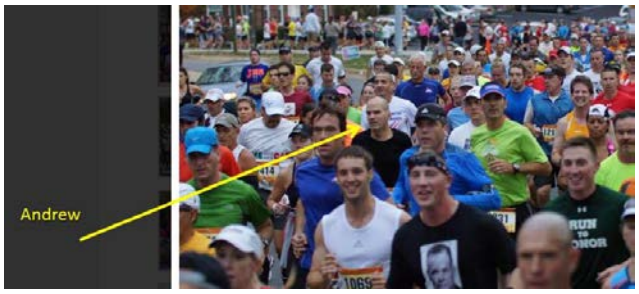

Figure 2: Facial recognition technology identified the author among more than 20,000 participants in the Marine Corps Marathon. October 2012.

There are multiple gathering and responder agencies. Traditionally these are local police, fire, emergency management (with the close assistance of GIS and IT), working as necessary with DHS, state and local homeland security agencies, the FBI, and FEMA. Increasingly these agencies draw on private resources such as security cameras and alarm systems. Networking needs to be flexible and able to quickly draw on resources outside firewalls without compromising security. As an example, the City of Baltimore made it possible, “on the fly” for private security cameras to be viewed inside their watch center by interfacing its fiber network with private systems in order to manage the Gran Prix and Sailabration events, as well as to manage crime fighting and be prepared for terrorist events.

Universities and academic institutions play an increasing role in public safety and both develop and host crucial data sets and applications for their first responder partners. Johns Hopkins Applied Physics Laboratory developed the Maryland and National Capital Region CCTV application. Towson University developed the Osprey GIS exchange. The University of Maryland developed and hosts the RITIS regional traffic management system.

One future vision for public safety applications is an "app shop" available to the broad public safety community, interoperable with existing devices and inexpensive. Universities are logical places for applications development, as well as testing, hosting, distributing and evolving the applications.

Public safety applications tend not to conform to a standard cloud or client-server approach, nor do they easily sit on a public-facing IP network. The need for security and privacy requires encryption at a minimum, and potentially also isolation of the user devices or servers. The need for availability requires system redundancies and a consistent, well-known network. Performance requirements may also require end-to-end packet delivery SLAs. A regional or research network would need to be prepared to accommodate these needs in addition to its more traditional applications.

A data exchange hub is one solution that has been used to create secure interoperability for diverse systems (CCTV, dispatching systems, GIS), with the hub sitting between different agencies or jurisdictions and dynamically providing access to data for properly credentialed users or allowing users to share data regionally. Data exchange hubs are costly and complex, but a fast, reliable network could enable a hub to be shared among a broad range of jurisdictions and agencies and minimize per-user cost.

Costs are growing, both for networks and applications. Individual interoperability initiatives (regional dispatching, GIS interoperability, radio system interoperability) cost between millions and tens of millions to develop, and all must be sustained through staffing, system management and software upgrades. The result is a growing gap between "have" jurisdictions and "have-not" jurisdictions. In the past, national grant funding such as DHS Urban Areas Security Initiative (UASI) grants have helped a wide range of jurisdictions deploy technology, but these are being reduced. Many grant-funded initiatives are now suffering because previously grant-funded jurisdictions cannot sustain what they have started, so initiatives must take advantage of any and all economies of scale.

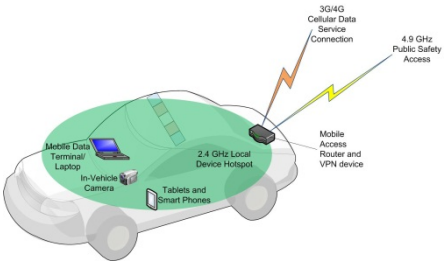

Figure 3: Typical public safety mobile broadband deployment, entailing multiple applications, devices, and network connections.

At the core of public safety interoperability is a talented cadre of leaders, administrators, and specialists. Frequently this core needs to balance their regional or interoperability roles against "day jobs" with their home jurisdiction. A strong network makes it possible for a team's limited time and energy to serve a broader base of jurisdictions and agencies.

Another area where regional and research networks can help is to reduce the long time to deploy a new system. As with the example of MAX, well-placed and secure infrastructure can reduce a three-year lead time in fiber construction to a few weeks. Current forecasts for the national public safety broadband network (NPSBN/FirstNet) are for a seven-year deployment, but existing fiber, data centers or development expertise may reduce this, or at least reduce costs.

FirstNet will require dedicated private, commercial carrier, and satellite systems. FirstNet will require extensive fiber optic backhaul, connectivity to data centers and emergency operation center,s and secure, hardened facilities for antennas. Currently the federal government has only funded a fraction of the total development and deployment cost, so considerable resources will need to come from resource sharing with commercial carriers and other entities. FirstNet would benefit greatly from innovative approaches and ideas (scientific, technical, operational and business/financial), since a "brute force" duplication of existing commercial networks is neither affordable nor advisable. The business model is still under development, but will likely require user fees, and therefore will pose the same challenge for sustainability as other public safety systems. Research and regional networks can play a part, by providing access to infrastructure resources (ideally, for a fee), taking part in development, and helping to create economies of scale.

Another future public safety initiative is next generation 9-1-1 (NG 9-1-1), planned to migrate 9-1-1 to IP technology, and allow interface to and from the system using text, email and video, and increase redundancy and survivability. Like FirstNet, NG 9-1-1 will require fiber optic backhaul, data center infrastructure, and innovation, as well as ways to reduce costs. Again, research and regional networks and the institutions that operate them can potentially make it possible to develop in an innovative and less costly way and help create economies of scale.