PUBLIC SAFETY ENTERS THE COLLECTIVE INTELLIGENCE ERA

HOW HIGH SPEED, MISSION-CRITICAL WIRELESS COMMUNICATIONS ARE HELPING FIRST RESPONDERS OVERCOME PUBLIC SAFETY ENEMY #1: THE UNKNOWN

BY PAUL STEINBERG, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MOTOROLA SOLUTIONS
It’s often said that what you don’t know can’t hurt you. But in public safety, nothing could be further from the truth. In fact, perhaps the biggest challenge first responders face is being forced to deal with the unknown. That means the biggest challenge a CIO or IT Director faces is how to make sure the right information gets to the right people, in the right way, at the right time. How to ensure every police officer, firefighter, EMT and dispatcher knows virtually everything important about every incident or situation. In other words, how to make the unknown, known.

COMMUNICATION OF INFORMATION

The answer, of course, is information. More specifically, the communication of crucial information to first responders to help them be more productive, more protected and more effective. We call it “situational awareness” and over the years both the quality of information and the ways it can be collected and communicated have improved substantially.

In the 1990s, the push was for communications technology that could get information in people’s hands to help improve personal productivity. This technology included personal computers and digital assistants. In the early 2000s, things changed. The objective became knowledge distribution, pushing information to everyone who needed it via connectivity to whatever mobile devices they had in their hands. By and large, this was a one-way data exchange from the command center to personnel in the field. Today, things are changing again.

THE COLLECTIVE INTELLIGENCE ERA

In the 2010s, we entered the era of broadband-enabled “collective intelligence.” The idea of collective intelligence is that everybody can produce and consume information. It is not simply pushed out to individuals in the field (like directed spokes from a hub), but shared among all team members and with disparate teams using two-way broadband communication technology. The goal is increased situational awareness. The reality is, each individual or team at an incident scene has a unique perspective on the location and can collect information that is unknown to others. Next generation public safety networks will make it possible for the “collective”—i.e., everyone on the team from dispatch to command to individual first responders—to both access and contribute to this critical information. In real-time.
SITUATIONAL AWARENESS

The idea of collecting and sharing information and intelligence is hardly new. As Bill Schrier, deputy director, Center for Digital Government, eRepublic.com, former CTO of the city of Seattle and one time police officer, notes, “Cops have done this forever, talking to people on the beat and to other cops, gathering and sharing information from a wide variety of sources. But now we can collect and share this intelligence using new social networking tools that allow collaboration among both Land Mobile Radios (LMRs) and broadband devices like smartphones and tablets.” What’s new is the ability to collect mission-critical information from a wide range of media and citizens—from 9-1-1 calls to street video surveillance cameras to sensors to information from a myriad of databases to on-scene, on-person video cameras—then share it immediately with anyone and everyone, including citizens en masse and in near real-time. It’s all achieved with powerful, secure, high-speed communications networks and the cloud.

MISSION-CRITICAL SOCIAL NETWORKING

Not coincidentally, the collective intelligence era correlates with the era of cloud computing and social networking. Both consumer and business customers are communicating and collaborating on sites such as Facebook, Twitter, YouTube, LinkedIn and scores of others. How widespread is the social networking trend? In October 2012, Facebook had more than one billion active users, over half of whom access the site on their smartphones or other mobile devices. YouTube is another example, with more than four billion video streams being watched every month.

With collective intelligence, we are essentially taking the social networking phenomenon and applying it to public safety in a structured way. The entire agency is communicating and collaborating in a social, interactive way over land mobile radio and broadband networks. Using the “cloud” as a data aggregation point, the most relevant, up-to-the-instant information can be made available to everyone on the network, in a secure environment. Public safety professionals are able to interactively collaborate over a variety of communications technologies and portable devices to bring up-to-the-instant knowledge to the response team as events evolve and are resolved. The cloud is also beginning to play an increasingly important role in other public safety applications such as disaster response and recovery. It allows individuals to collaborate and share various assets such as floor plan maps.

PUBLIC SAFETY AND SOCIAL MEDIA

Recent statistics from the Washington, D.C.-based Police Executive Research Forum tell the story:

- 83% of police agencies use social media to share information with the public.
- 70% use it to receive tips from the public.
- 89% use it to monitor investigative leads.

Smartphones are expected to generate more mobile data traffic than all laptops, combined, for the first time as soon as 2013.

- Cisco Systems
What does collective intelligence look like in the real world? A SWAT team dealing with a hostage situation, for example, can use two-way streaming video for communications and collaboration. High performance bi-directional communications allow the “feet on the street” to not just access the collective, but dynamically contribute content to it. Video is captured on the scene by officers on the ground, in vehicles or helicopters. Cameras can be placed on mobile robots that actually go into the building and stream video back to command. These constant feeds of images and information from different perspectives are streamed to the on-scene mobile command unit. The team leader then directs the video feeds to provide responders with the most relevant information, and disseminates the video to whoever needs it—including sniper teams—to enhance safety by enhancing situational awareness.

Collective intelligence is just as critical on a fire scene, for example, at a chemical plant. To begin with, the incident command center and individual firefighters can access a wealth of real-time information on their wireless broadband devices such as ruggedized handheld computers. Each team member can have immediate access to building details such as floor plans, sensor inputs, location of electrical panels and the types and locations of hazardous materials. They can also get clear audio communications, as well as streaming video from various angles and perspectives. When the incident commander in the mobile command center views live footage from a helicopter, he sees what the team on the ground can’t see: that the cut they’re about to make to vent the roof is being made in a less than optimum place. The commander annotates the video to the team leader, who moves the venting operation to a more effective location.

Collective intelligence is also essential for Emergency Medical Services (EMS) technicians to move data real-time between the ambulance, the hospital and in some cases a medical dispatch center. Patient data can be gathered from various medical devices, centralized on one screen at the back of the ambulance and shared in real-time with incident managers and emergency room doctors who can begin treating the patient before he arrives at the hospital.
ENABLERS OF COLLECTIVE INTELLIGENCE

How are public safety CIOs preparing their operations for implementing these vital new collective intelligence solutions? Most start by reviewing and reassessing their plans for the era’s most important enabling technologies: reliable, high-speed broadband networks; tough, easy-to-use mobile devices; and innovative public safety applications that help empower every member of the collective.

BROADBAND NETWORKS. Public safety departments understand that the foundation of their high-speed data communications is a mission-critical wireless broadband network. This network needs to deliver the coverage, speed and reliability—as well as interoperability with P25 voice systems—to support true collective intelligence. Since reliability is so crucial for public safety, CIOs recognize the importance of implementing a privately owned network that’s built from the ground up to be mission-critical. What kinds of networks are public safety departments opting for? Today, there is strong momentum behind Long Term Evolution (LTE) networks as the preferred broadband technology for public safety use cases worldwide.

PORTABLE DEVICES. In addition to infrastructure, public safety CIOs are also considering the specific types of mobile devices they wish to utilize, not just for today, but for the life of the network. They’re looking closely at ruggedized, ergonomic, intuitive wireless devices—from powerful in-vehicle technology to ruggedized handheld first-responder computers—that help connect, inform and protect every member of the collective. They can be confident that their standards-based LTE networks will support both current devices and the innovative new devices of tomorrow.

PUBLIC SAFETY APPLICATIONS. Open-standards LTE networks also support the fast-growing portfolio of innovative, productivity-enhancing public safety applications now being developed all around the world. Especially important are powerful multimedia applications that can combine voice, data and video to power the benefits of collective intelligence. Some of these applications are Computer-Aided Dispatch (CAD), analytics, streaming video, still photos and illustrations, facial recognition software, next generation 9-1-1, access to large maps or data files, work ticket management, automated license plate recognition and more.

PREPARING FOR FIRSTNET

At the same time public safety CIOs are planning for the collective intelligence era, they’re also preparing for inclusion in FirstNet, the nation’s proposed coast-to-coast interoperable public safety broadband network. Although still in the planning and decision-making phase, FirstNet will ultimately enable first responders in every part of the country to communicate and collaborate with others in times of statewide, regional or national emergencies or weather-related disasters. Fortunately, for most departments, these preparations follow parallel tracks and utilize the same technologies, devices and applications. The movement to standards-based LTE broadband networks for collective intelligence operations has much to do with the fact that LTE has also been designated as the network technology standard for FirstNet.

“We want to be able to collect a complete picture of an event by amassing information from a wide range of sources,” says Jeff Johnson, CEO of the Western Fire Chiefs Association. “We then share this collective intelligence by pushing the information back to the field.”

It’s all about eliminating, or at least considerably reducing, the unknowns. The more public safety officers know about a situation—profiles and photos of suspects, streaming video of the actual location, area maps, building plans and more—the safer and more effective they will be. And the safer the community and its citizens will be.
ELIMINATING THE UNKNOWNS

Bottom line, collective intelligence systems help save first responders and the public from the dangers of the unknown. Here’s how the concept of collective intelligence helps in the examples discussed at the beginning of the paper.

• As the car is being pulled over, the dashboard camera scans the license plate and the system automatically sends the data to the statewide database revealing a long history of traffic offenses. Then, before exiting her vehicle, the officer receives information that 20 minutes ago the driver was involved in a domestic violence incident and should be presumed armed and dangerous. She calls for backup and her in-vehicle workstation shows her when and where the backup will arrive. In moments the team of officers has the suspect in custody. And all the activities have been monitored and sent in real time to the command center and dispatch.

• Officers responding to the “shots fired” call are able to immediately access streaming video of the scene from street video surveillance cameras, including those of private businesses, gaining real-time situational awareness that enables them to take a safer route to the incident, avoiding any crossfire. A contingent of backup units is also able to access the video on the network. In addition, officers are able to see video of the fleeing suspects taken from a citizen’s mobile phone, making it easier to identify them and make the arrests as they try to escape. No one is injured. Overlaying the first responders (vehicles and individuals) on a map or floor plan that can be seen by all participants allows for a coordinated and orchestrated effort to cope with the incident.

• Before entering the burning warehouse, firefighters are able to confer with responding utility crews regarding the building’s electrical systems. They access current building plans both on their in-vehicle workstations and handheld computers. They are made aware of the hazardous material storage location, enabling them to better assess the situation and quickly move to extinguish the flames before they reach the storeroom. With no explosion to increase the fire’s intensity, scope and peril, firefighters are able to contain the fire to a single floor with no serious injuries and minimal structural damage.

Collective intelligence is clearly a future paradigm enabled by technology. We can only start to imagine how it will play out based on advancements in broadband networks, portable devices and public safety applications.