John Maher warns secure radio communication technology could offer a tactical edge to both responders and terrorists alike and calls for greater inter-agency interoperability

FREEDOM OF SPEECH

The Paris attacks on the *Charlie Hebdo* publication office in January 2015 is evidence of a new profile of terrorism, furthering the reality that, despite ongoing, aggressive intelligence gathering, terrorist attacks will occur due to the sheer volume of information, noise filtering, geographic reach and evolving plots. Terrorist organisations are becoming better funded, trained and prepared. When an attack occurs, it can be completely unpredicted and the method, location and purpose unknown. Law enforcement must be ready to respond to a range of attacks at all times to prevent or minimise loss of life and property. Effective tactical response is critical to stopping, minimising and recovering from terror events. Law enforcement must be better prepared, equipped and co-ordinated than the terrorist. Interoperable secure communications provide critical situational awareness and co-ordinated, rapid response for law enforcement across jurisdictions and agencies.

Radio systems are ideal tools for first response law enforcement because they are inherently flexible. Radio communications have the ability to be ad-hoc, independent of any network infrastructure, always available, highly mobile, and secure. Radio costs have also decreased while performance and functionality have improved. But because of the cost/functionality evolution of radios, buying a secure radio is no longer restricted to government or military. The same performance capabilities and cost reductions make secure radio systems attractive to, and within economic reach of, terrorists – even those with just a modest financial support network.

For law enforcement to gain a superior tactical edge against terrorists with secure communications in a crisis scenario, few options exist. Lawful intercept is not possible for radio – radios do not have the analogous infrastructure that enables such a capability. Though radios are relatively trivial to monitor, the security in them is end-to-end – there is no service provider delivering the privacy overlay that can be tapped to provide either user communications or the associated metadata. The broadcast nature of radios means that radio transmissions are easy to tap, but strong encryption technology makes it near-impossible to decipher the communications. Law enforcement is left with more limited capabilities such as jamming or radio location to keep the tactical edge.

Many governments around the world regulate radio systems that are sold in their jurisdictions to ensure capabilities to defeat law enforcement action are limited. Certainly, the regulation of products sold within jurisdictions is a long established precedent used for a wide variety of purposes such as ensuring consumer safety, protecting indigenous industry, mitigating environmental concerns and regulating frequency spectrum, among others. Government regulation could dictate that law enforcement had the technical advantage by ensuring that commercially available radios had limited performance and security capabilities. Current widespread import regulations for managing the radio spectrum could be enhanced to control other aspects of radio operation such as cryptographic key strength, modulation waveforms, or other performance characteristics.

As a practical matter, however, it is unlikely that such regulation would deter the motivated and well-supported organisation which wanted to ensure its operations would be immune from law enforcement visibility. Secure radio systems can be physically small, and easily hidden and transported. It would be easy enough for these radios to be smuggled into any jurisdiction without detection, especially if the adjacent jurisdiction did not have a similar level of control and enforcement. Once inside the country, the secure radios can be deployed to support whatever the user's needs are before law enforcement can detect or in some way prevent their use.

So, how can law enforcement ensure effective communications to maintain the tactical advantage? It is incumbent on law enforcement to ensure they not only have a secure communications solution deployed with their radio systems, but also one that is interoperable across agencies and jurisdictions. This ensures that, from a communications point of view, they have tactical superiority inherent in the ability to communicate freely with all forces to counter terrorist activity. Even if their adversaries are also deploying secure solutions, law enforcement will have the tactical edge due to these communications.

Despite the deployment of interoperable secure communications appearing to be an obvious approach, law enforcement and intelligence communities face challenges. Establishing interoperable solutions for radio in law enforcement is subject to the constraints of budget cycles, sunk costs in current radio systems, and non-co-operative bureaucracies that have their own disparate technical requirements. These barriers mean that concerted effort must be made to ensure these secure, interoperable solutions exist and are deployed. The simple economic solution may be to deploy an external radio encryption add-on that allows existing radio systems to communicate securely, independent of the radio equipment, without impacting existing radio applications.

Given that the interoperable secure radio solution must


DESAUTEL

©Getty Images

Secure inter-agency communications provides law enforcement and first responders with a vital tactical edge

be put into action quickly across various agencies and jurisdictions and in the midst of a crisis, usability and ease of deployment and management are also critical. Even if radio systems have a common technical capability, they are generally deployed with agencies that have their own independent daily mission. When an event occurs that requires a co-ordinated response, these systems must go from independent operation to unified communication so the different law enforcement or military agencies can securely communicate.

There are several logistical considerations that must be co-ordinated to ensure radio systems which are typically used independently are ready to interoperate. Communication hierarchies based on command structure will have to be pre-established and users trained. Radio configurations will also have to be preconfigured or established and tested to ensure a smooth transition. Ensuring cryptographic compatibility between the systems through co-ordinated key management is another important factor. Since there are several encryption key distribution methods and systems, the key management system will have to be designed to support the transition to a unified communications environment where the necessary security overlays onto the communications hierarchy.

A centralised key management scheme enables singular control of the key generation and distribution, providing the best opportunity for co-ordinating the security to match the communications hierarchy. It also allows for maximum compartmentalisation so the risk of compromise in the key management mechanism is minimised. Mitigation of potential issues of scalability, which are characteristic of many centralised control systems under dynamic environments, will need to be considered. A centralised control scheme also needs to address the potential for single point of failure, especially when the system is under stress.

Fortunately, these issues can be addressed logistically if there is prepositioning of configuration and cryptographic keys before the need arises. Once an event occurs and unified response is required, the command hierarchy can trigger the pre-planned transition of the communications system security. An alternative key management solution is the distributed key management system where keys and configuration are locally generated and distributed. Distributed systems resolve the issue of scalability but introduce other considerations. The issue of interoperability in the distributed key scheme needs to be considered to assure secure communications can be established between the appropriate agencies with their own keying systems. In this case, some level of centralised organisational control has to be pre-established to ensure the distributed security systems are co-ordinated. This hybrid key management approach ensures that concerns of both scalability and co-ordination can be resolved while still maintaining compartmentalisation critical to highly secure communication systems.

Radio has no bounds of flexibility. Local, inter-state, inter-agency, across borders and over land, air and sea, law enforcement and military can securely communicate. With the right radio security infrastructure, these communications can be interoperable, co-ordinated and secure from end to end. End-to-end security means signals are always encrypted from user to user – never decrypted in intermediate network points which create security risks.

Secure radio communications are becoming more available, more widespread and are reaching the hands of terrorists. At the same time, radio networks by their broadcast nature do not enable lawful intercept capabilities. While intelligence gathering to counter terrorism is ongoing, some events will occur without forewarning due to the volume of intelligence, noise filtering and evolving plots. To be ready for these inevitable events, law enforcement must be prepared with secure radio communications that are quickly interoperable across agencies and jurisdictions. The radio solutions must be easy to use and manage to give law enforcement the tactical edge with full end-to-end security to protect the safety of law enforcement and citizens.

John Maher
is director of Engineering and Product Development at Technical Communications Corp, a global provider of secure communications systems, solutions and services. He has more than 20 years of experience in cryptography, network communications and military systems, and holds an MSCE from Renssalaer Polytechnic University as well as a BSEE from the University of Connecticut.