John Maher argues that secure, interoperable radio communications are essential for effective counter-terrorism operations and calls for more flexible solutions

COUNTER TE

All major disasters – from hurricanes to industrial accidents and terrorist attacks – require co-ordinated emergency response. Depending on the scope and incident, the co-ordination must span across local and national agencies. Being prepared is the key to effective, timely and co-ordinated response, including having in place appropriate communications channels and processes.

The magnitude and frequency of natural disaster scenarios are difficult to predict, but they follow the laws of science and past history serves as a guide to possible future events. With this information, response teams can map contingency scenarios, establish a leadership hierarchy, train for events, and pre-arrange communication channels.

Terrorist attacks, on the other hand, follow no physical laws and no predictable path of behaviour. Terrorism strikes, by their very definition, are often unexpected, and their scope and scale unanticipated. Security personnel charged with protecting life and property are left trying to predict without precedent what may happen, with no knowledge and few tools. The attacks on the World Trade Center

RROR COMMS

and Pentagon on 11 September 2001 established a new unforeseen scale in the evolution of terrorist attacks. When the US government realised that the total scope of the co-ordinated attack was unknown, the Federal Aviation Administration took the unprecedented step of grounding all flights in or headed to the United States.

Even though terrorist attacks are of unknown scope and duration, an effective, co-ordinated response can disrupt the attack plan and its execution. To do this, a larger response beyond local authorities is often required. Disaster response requires interagency co-ordination for the flow of information necessary to protect its citizens. As such, effective voice communications are essential. While all crisis response situations demand effective, co-ordinated communications, terrorist events also require communications to be secure.

The initial response to a terrorist attack often occurs during the actual attack when both terrorists and security personnel are operating in a localised tactical environment. In this environment, the advantage goes to the side that is more tactically aware and can anticipate or know the actions of the other. These requirements dictate that the communications be mobile, ad hoc and, most importantly, secure. The extensive application of secure voice communications among the response forces is essential to maintain or gain that tactical advantage. For these forces to be able to operate with privacy, a tactical level of communications security is sufficient. The information that is exchanged in these operations is of short-term value and the adversary is not a well-resourced national agency capable of sophisticated real-time exploitation. This simplifies the requirements and the cost of a communications security solution. Higher-level strategic solutions can obviously work in such a scenario, but these solutions generally come with higher investment and operational costs.

It is clear that for security personnel, mobile, ad hoc, secure radio communications are needed to provide the necessary tactical advantage for response to terrorist threats. Radio channels are more resilient to disaster and are typically the channel of choice for homeland security and military forces. The challenge is that secure radio solutions that interoperate across local and national security response teams often do not exist. It is typical that forces representing the various police, paramilitary, or military forces within a country have radios of varying generational origins and manufacturers. This disparity is a natural consequence of the various missions, funding levels, and government bureaucratic structure. Until a major event occurs, such as a large-scale terrorist attack, there is little motivation to establish communication systems with interoperable security.

The issue of common communications systems has been difficult to resolve for a number of very predictable reasons that are technical, administrative, and political. The technical requirements are typically very different. Local law enforcement, whose area of coverage is geographically limited, would be unlikely to deploy a radio system with the mission capabilities required by military personnel. As a decision maker in the law enforcement community, the responsibility is to provide the best technical solution at the lowest possible cost. That means providing radio solutions that are optimised for the very specific requirements of daily law enforcement operations within the department. These radios are likely to be inexpensive, have limited functionality and are often not secure. This is in contrast to military radio systems designed to support an entirely different mission requirement of defending its borders from threats.

A secure interoperable radio solution is difficult to achieve even in a single department. Older generation radios may not have a built-in secure communications feature, making any radio with a voice encryption feature incompatible in a secure mode. Radios with a voice encryption feature historically have had proprietary security solutions that do not interoperate between suppliers, even when specified in the same frequency bands and modulation techniques. In this case, users looking for interoperability are forced to use them in a plain (unencrypted) mode of operation, compromising operation security.

Besides the technical barriers to interoperable communications systems, the specification, budgeting, procurement and deployment of communications systems independently by the various government agencies is a challenge to the need for interoperability. Even organisations as motivated and resourced as the US Department of Homeland Security (DHS) have struggled with a solution. The problem of the various local, state, and federal government agencies within the New York area using incompatible radio communication systems was addressed as a priority issue in the wake of the 9/11 attacks. The DHS took the approach of working to create a common interoperable radio channel and purchasing standardised equipment department-wide. But as recently as November 2012, the US Department of Homeland Security's Office of Inspector General reported that despite a $430 million investment, "… DHS had limited interoperability policies and procedures, and component personnel did not have interoperable radio communications". The reasons this has not been resolved are various, but illustrate the magnitude of the challenge. For government agencies that are not so well resourced and funded as the DHS, the standardisation and procurement of a single standard is therefore not practical.

The DHS case illustrates the obvious solution to

interoperability: specify a single system and deploy it across the entire population of users. But the DHS case also shows that such an approach can be a significant hurdle for governments that are not deeply resourced. There are a couple of approaches to resolving the interoperability issue which provide the essential capability but with lesser commitment in terms of resources and cost. The first is to go to a single vendor solution based on an existing standard for initial deployment and then growing the system in an evolutionary fashion. The second is to consider a security overlay to existing radio inventory, which allows secure interoperability between multiple vendors and generational radios.

In service today are two major standards for radio communication systems targeted at public safety and other government agencies. In North America, Project 25 (P25) standard is commonly deployed, while the Terrestrial Trunked Radio (TETRA) is used in Europe and considered to have a more global reach. Each has advantages, but both can be considered to serve a similar capability. Both of these systems provide an encryption capability to secure voice and data transmission. To deploy effective encryption key management, add-on encryption systems may be required, however. These systems can be complex to deploy and manage, requiring investment not only in the key management systems but also training and ongoing operational costs. Both of these systems are supported by several major radio manufacturers who can supply turnkey solutions. This still requires significant technical understanding to oversee the specification and procurement to ensure recommended systems meet operational, maintenance, and security requirements and expectations.

For security agencies that are limited in resources or need a near-term solution, a security overlay can provide the necessary capability to secure communications with minimal impact on existing equipment or infrastructure. This solution is implemented as an in-line encryption device that is applied between the handset or headset and the radio itself. The solutions come with their own key management systems and are relatively easy to manage. Depending on the device, these systems can be very simple to deploy and use, requiring little training of the end user. A drawback to this solution is that another device has to be procured and inventoried by the agencies involved. The device also has to be carried or body-worn by the user or mounted in vehicles/aircraft/ship/command station, creating an additional size and weight penalty.

The advantage of an external appliance is that it can be selectively deployed in small numbers for situations that require secure communications. This means that an investment in a small number of these devices allows them to be deployed on-demand wherever a need arises as part of an interdepartmental secure communications solution. An external secure radio appliance can also be used to extend security to existing radio inventory, or add to new radio inventory over time. As existing infrastructure is used, a security overlay can also be incrementally more cost-effective.

Terrorist threats and attacks are today's reality. They present a unique challenge to security personnel charged with maintaining the safety of it citizenry. The unknown scope and duration of these attacks means there is a need for mobile, ad hoc, secure communications to effectively respond to and counter terrorism. Tactical encryption of radio communications provides security teams with the ability to communicate privately and maintain the advantage over even well-prepared terrorist groups. Given that interoperable secure radio communications do not exist due to the nature of varied departmental requirements and compartmentalisation of governmental procurement, a solution is needed to provide this secure interoperability to security forces. Two major solutions exist. The first is to establish policy and attempt to deploy standards-based radio systems such as European TETRA or North American P25. Such a solution provides assurances of interoperability as well as new system capabilities but still requires in-house system engineering capability, and investment in infrastructure, equipment, and training. The second solution is to provide a common external encryption device that allows existing inventory radios to interoperate securely. While an add-on device requires additional equipment to manage, these relatively simple solutions are flexible and easy to deploy, make the most efficient use of existing inventory investments, and provide a more immediate and affordable solution.

©Getty Images

Attack and response: a security overlay can provide secure communications with minimal impact on existing equipment or infrastructure

John Maher is Director of Engineering and Product Development at Technical Communications Corporation. For more than 50 years, TCC has been securing voice, data and video communications for military forces, government agencies and corporations worldwide.