Voice Privacy and Security

As nations work to improve their national defense strategies, many are seriously examining their current radio communications infrastructure.

By Mike Kelley, General Manager, Transcrypt International

For more than 50 years, the nations involved in the economic organization known as the European Union have had one main goal — to promote economic and social progress. In recent years, the organization has reached significant milestones, including the introduction of the euro and the formation of a single economic market, which has further asserted Europe's leadership internationally. While this exchange of information across borders is a significant evolutionary step in international business, it brings with it a burgeoning security concern for governments and their agencies.

The effects of Sept. 11 have reached beyond the United States, and nations around the world are intensely focused on national security and their own homeland defense efforts. Governments are taking steps to empower agency personnel with the ability to communicate securely and share information efficiently. Occasionally this requires governments to develop a plan for communications with neighboring countries that provide for cross-border cooperation.

As nations work to improve their national defense strategies, many are seriously examining their current radio communications infrastructure to determine whether it will meet demands on two fronts — voice privacy and interoperability. Voice privacy technology scrambles critical communications to keep out eavesdroppers, enabling information to be securely shared. Interoperability allows multiple jurisdictions to communicate and share information, which aids a nation's public safety community both tactically and strategically.

Voice Privacy Focuses on Flexibility

Providers of voice privacy solutions report an increased interest among potential customers in various scrambling technologies, despite the fact that a number of new vendors have entered this market over the past two years. Governments that plan to update their voice privacy solutions should look for a company with a proven track record of innovation.

For voice security, reliability and dependability are key to risk reduction. After-market scrambling modules can be added to radios used in the field at a fraction of the cost of new radio infrastructure or subscriber units. While at the international level this market is rather mature, growth opportunities still exist for companies offering solutions that feature multiple capabilities in systems management, security management, and flexibility.

Managing systems inefficiently is a major liability for a law enforcement agency or a paramilitary group. For example, agencies sometimes have to bring radios into a maintenance shop and physically connect them via cable to make any changes. One of the key developments in encryption systems management is remote management capabilities. Over-the-air rekeying (OTAR) allows for remote management of scramblers. Systems managers can update security codes in a secure manner from a centralized office location that has access to the radio systems, similar to a dispatch center.

Additional systems management features to consider include automatic number identification (ANI), a tracking mechanism that provides information about who is transmitting in a particular time period. Agencies should also consider selective calling, which allows a dispatcher to call a particular unit and let them know that someone is requesting a transmission.

Scrambler and security management features in encryption solutions offer agencies the ability to change security parameters on a regular basis to ensure that information remains secure. When a system becomes impaired or an unauthorized person acquires an encrypted radio, scramble code management allows for a forced scramble code change across the system. Some scramblers have the ability to hold up to 16 codes at once in their memory. These codes can be changed one at a time or all at once, across single units or multiple units. Thus, managers can request acknowledgements from the scrambler to verify that it is active and has valid security codes. If an agency official suspects that an adversary has appropriated a radio, a radio-kill feature enables remote disablement of the radio via OTAR to prevent a security breach.

Because many radio system limitations are the result of how the radio infrastructure was first implemented, government agencies, first responders, and law enforcement/military organizations should look for solutions that offer maximum flexibility. Flexibility features for encryption modules include button reassignment and emergency signaling. The scrambler mode selection, for example, can be made from an assignable radio button, allowing users to easily switch between clear and coded transmissions.

Radio communication investments can be expensive, and field personnel need to be able to use all the features of their radio systems without experiencing interference with the scrambler on the system. When selecting an encryption solution, it is important to know that only a few providers offer the full gamut of these features to international government customers. Even though many of these features are not really necessary, providing all of them in a single package allows users to manage the system and security while providing flexible functionality.

Solutions should also be upgradeable. A nation can stretch its money by initially purchasing a low- or medium-security solution and later upgrading to higher security when threats increase or budget allocations become available. Some providers offer a flexible upgrade pass that customers can use to upgrade to a particular encryption level at a later time.

The strength and reliability of encryption solutions are often put to the test. Military applications require frequent changes of security codes due to more sensitive applications. One international customer using OTAR functionality, for example, no longer has to bring in the troops to central stations to change codes after purchasing a versatile scrambler.

Interoperability Promotes National Cooperation

As nations begin to task government agencies with working together in more cooperative ways, radio communications interoperability will play a significant role in making this happen. It is unfortunate that we must continually look to Sept. 11 as the driver of change in public safety communications, yet the events of that day revealed the shortcomings in both strategic and tactical communications interoperability around the world.

Radio infrastructure is fairly costly and takes time to establish; the option of building out new infrastructure is not one to be taken lightly. It requires significant planning, and in most cases, agencies would not see a complete change-out of hardware on a frequent basis, similar to what occurs in faster moving technology markets such as personal computers.

As an alternative to full infrastructure upgrades, many land mobile radio manufacturers have developed tactical interoperability solutions. Rather than requiring a full build out of interoperable radios and repeaters, these solutions can be used in the field immediately and are compatible with almost any radio system. Many Latin American nations have expressed interest in these types of solutions due to their inability to build out the complex infrastructure necessary for truly interoperable solutions.

Plug-and-play interoperability devices offer the simplicity of plugging in cables at one point and radios at another to communicate over disparate radio frequencies. During a police incident or forest fire, the issue is how quickly a system can be made interoperable. Are you ready in minutes, hours, or days after plugging radios into an interoperability command center, programming it, and getting everything set up?

Here the savings are not only in cost, but also potentially lives and property. The most critical time for interoperability is at the very beginning of an incident; tactical interoperability solutions provide an advantage right from the start, in a matter of minutes. Another benefit of these types of solutions is the ability to provide a quick, easy way to extend range. By doubling the range of one radio, it can act as a simple repeater, which is attractive to many international agencies.

It makes sense for smaller nations that occasionally work with neighboring countries to invest in simple and cost-effective interoperability kits rather than expensive and permanent interoperability infrastructure. A small country's national security force or police force may need to temporarily interoperate with a neighboring country due to a threat from a common enemy or a border incident. Naturally these nations do not operate on the same radio frequency and will need assistance in achieving interoperability.

Where Do We Go From Here?

In the past few years, a system-level discussion about Project 25 interoperability standards has dominated the United States, yet many nations around the world have not embraced Project 25 as an interoperability solution due to its high infrastructure costs. Instead, many solution providers have focused on strengthening the features and functionality of after-market voice privacy modules.

International law enforcement officials and other public safety workers have had their hands full just dealing with the new threats each day brings, and governments are focused on providing reliable and flexible encryption and interoperability solutions to these users. They are starting to recognize the urgent need for collaboration, however, which will usher in a new era of information sharing to aid homeland security in the United States, Europe, and around the globe.

Mike Kelley is General Manager of Transcrypt International, a subsidiary of EFJ Inc., a provider of interoperable wireless communications systems and voice security solutions for government agencies involved in public safety and homeland security. Contact Kelley at mkelley@transcrypt.com.

RadioResource International delivers wireless voice and data solutions for mobile and remote mission-critical operations. The magazine covers private and commercial mobile radio, wireless data, public safety communications, microwave radio, satellite communications, paging/messaging, and other wireless applications. Editorial content is international in scope and encompasses news, standards, new products, emerging technologies, industry trends, and troubleshooting tips.

To request a FREE subscription or get more information, go to www.radioresourcemag.com.

RadioResource International is published by Pandata Corp, 7108 S. Alton Way, Building H, Centennial, CO 80112, Tel: +1 303-792-2390, Fax: +1 303-792-2391, www.radioresourcemag.com.