
# A Call for Preparedness

## Communications Issues You May Be Overlooking

By Megan Hein

In a world where cultural, religious and border conflicts can cause extremist groups to act maliciously, it can be exhausting to think about the vast number of ways a terrorist organization could violate the security of a nation. As America examines its borders, ports, airlines and more, we realize it's impossible to be completely immune from terrorists, which is why every appropriate agency must do everything in its power to protect its citizens.

In a hypothetical scenario, imagine thousands of emergency professionals gathering in a large southwestern city for a three-day conference and expo. The city and venue would certainly take extra security precautions to protect the safety of the attendees, requiring identification badges and parking passes, and using security guards to control access and inspect bags. State and local police would provide security for the event by patrolling the area around the clock both on foot and by automobile, validating all service workers and vehicles.

A day into the conference, however, attendees begin to get extremely ill. Many start vomiting, having seizures and complaining of diarrhea. Some simply return to their hotels, but others begin arriving at nearby emergency rooms. It's clear that something is terribly wrong as hospitals are becoming overwhelmed and the situation becomes more desperate by the hour.

The media picks up on the story by listening to police scanners and begins to swarm the area, reporting the story —including the names of victims— before any official information is made available.

To respond to the situation, the Department of Homeland Security needs to communicate its strategic response plan to emergency response personnel, but the agencies' analog radios are not interoperable. That means the police, firefighters, emergency medical technicians, FBI, Department of Health and Human Services, Red Cross and other agencies can't communicate with one another via radio. Patients found by police don't get immediate medical attention, Red Cross volunteers can't request needed supplies, and efforts to find the source of the attack are being duplicated by multiple agencies.

### The attack

After much analysis, investigators discovered the source of the attack was ricin, a poison made from the waste of processed castor beans. As it happened, a terrorist cell planted a member with the catering company hired to prepare meals at one of the booths. In the days leading up to the show, the terrorist organization learned the ins and outs of the conference's security measures by eavesdropping on unsecured analog radio communications via a scanner purchased at a local radio store. They learned that service vehicles would be given a physical inspection, so they chose an easily concealable method of destruction. They were also able to determine when the security checkpoints would be understaffed and what types of vehicles officials were most concerned about from a security standpoint. Separately, these bits of information may seem trivial, but small pieces of intelligence such as these add up quickly.

The morning of the show, the undercover terrorist switched out a small container of sugar for a similar container of ricin, adding small amounts of the poison to coffee, tea and other beverages. In addition, the insider information they had gathered from unsecured analog radio communications allowed the terrorists to stay a step ahead of every security precaution at the conference. The scanner allowed the terrorists to be aware of every move officials made to track them down, allowing them to evade capture. Furthermore, using a similar scanner to monitor analog radio conversations, the media was able to gain valuable and confidential information about the incident. This led to the premature release of victims' names, a violation of Health Insurance Portability and Accountability Act (HIPAA) regulations, and the exposure of the emergency response agencies'

lack of preparedness.

## Would you have been ready?

The use of voice encryption and radio interoperability products would have drastically changed the outcome of such a scenario. Even the most innocent-seeming information transmitted through analog radio communications can be of utmost value to someone planning an attack. By using an inexpensive scanner bought at an electronics store or simply listening to radio dispatch on the Internet for free, criminals and other unwanted listeners have the ability to eavesdrop on unsecured analog radio communications and thus use that intelligence to their advantage. It is for this reason that two-way radio communications must be secured by voice encryption products.

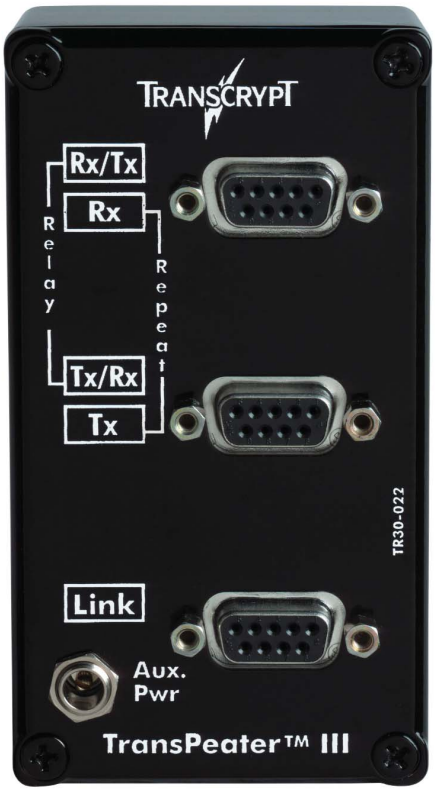
The only way to prevent sensitive information from being intercepted by unwanted listeners is to utilize voice encryption products—or voice scramblers—that protect radio conversations from eavesdroppers. With voice encryption modules, analog radio communications can be secured and only those with authorization will be able to communicate.

The radio interoperability problems can easily be prevented, but too many communities are still being put at risk because of them. As more unconnected agencies become involved in an incident, precious time is lost because radios operating on different radio bands and frequencies cannot connect. Perhaps a more calculated response plan would include the use of a portable cross-connect unit, which would have enabled otherwise incompatible radios to communicate.

Since the dependability of voice security and interoperability products can mean the difference between life and death, it is important that the products are reliable. Although cost should naturally be taken into consideration, the quality and type of security needed ultimately surpass price when it comes to such significant matters. Important considerations are to ensure that the products come from a company that provides proven solutions, thorough training and a solid reputation. There are different voice encryption modules available for varying levels of need—the product manufacturer or dealer should be able to assist in determining which level of security is appropriate for your requirements.

An underground terrorist organization could be operating where you least expect it, as are gangs and other criminals that could benefit from listening in on your transmissions. Fortunately, there are voice encryption and radio interoperability products available that can be utilized to help prevent and/or contain their actions. When the unexpected happens and that worse-case scenario presents itself, and it's your emergency response plan that needs to save the day, ask yourself again, "Would we have been ready?""

*Megan Hein is a marketing intern for Transcrypt International, a worldwide leader in voice privacy products. For more than 27 years, the company has provided scramblers, signaling, programming and interoperability products to meet the varied needs of land mobile radio users around the world.*




**When used in relay mode, Transcrypt's TransPeater III can connect otherwise incompatible radios.**