

# Training Exercises

Dale Ferriere and Payton Garbarino

NI<sup>2</sup> Center for Infrastructure Expertise

## Tracking – and slaying – a Trojan horse

Because of their potential vulnerability to being used by terrorists, intermodal cargo containers have been described by U.S. Customs and Border Protection as the potential “Trojan Horse of the contemporary century.”

A cargo container could be used to deliver a weapon of mass destruction, or the components of a WMD, directly to America’s heartland from anywhere in the world. The resulting disruption to the supply chain (ship, rail and truck) could have a catastrophic impact on the U.S. economy.

With this scenario in mind, projects such as CBP’s Operation Safe Commerce have focused on ways to use technology to secure, track and monitor cargo containers and their contents. [Ed.: See “Safe harbors,” October 2005.]

But tracking and monitoring containers is just one aspect. What happens when a monitoring device detects a problem? Who decides whether there really is a problem? Who gets notified? How is data transmitted to law enforcement agencies and other responders?

And in light of the 9/11 Commission’s criticisms on the need for improved interoperability between federal, state and local agencies, will existing protocols and procedures enable responders to pre-empt a cargo container’s use as a weapon of mass destruction?

### The exercise and its objectives

Looking toward the future when everyday use of smart container technology becomes a reality, last November the National Infrastructure Institute’s Center for Infrastructure Expertise (NI<sup>2</sup>-CIE) <www.nizcie.org> ran a real-time exercise testing the ability of commercially available geo-position tracking devices to enhance intermodal cargo container security and to link this tracking data with first responders and their information networks, possibly thwarting a terrorist attack.

The exercise’s overall objective was

to design and execute a series of tests to simulate a cargo container’s tracking device in “alarm” condition. For each test, a public emergency notification system was alerted. The response protocols of each notification system were evaluated to determine what gaps, if any, exist in the communications interoperability between the cargo container supply chain and the public safety environment.

The exercise was also intended to:

- Perform phone surveys and site visits at selected local, state and federal emergency communications and anti-terrorism centers to evaluate existing interoperability protocols.
- Test a law enforcement information network as a possible communications link for transmitting smart container data to federal, state and local law enforcement and other first responders.

Commercially available tracking devices suitable for intermodal container and over-road transport applications can:

- monitor geographical position (latitude and longitude),
- display the device’s position on an electronic map,
- track the device’s over-road route,
- provide on-line secure access to the device’s location information and
- provide geo-fencing (see below).

In addition, some devices can remotely shut down the truck that’s transporting the container.

After evaluating several off-the-shelf tracking devices, NI<sup>2</sup>-CIE selected a GlobalTrak test device because of the technology’s reliability and because a support technician was available locally to assist in the testing. <www.wcclp.com/Products/Iridium/MariTrack\_Vessel\_Tracking/>

Included with these tests was a demonstration of the tracking device’s “geo-fence” capability. Geo-fencing is a feature that stores geographic boundary information on the tracking device.

When a stored boundary is violated, the device will notify the user by having an alarm sent to their e-mail, fax, phone or pager. A geo-fence can also be plotted on an electronic map.

### The scenario

Northern New England was chosen as an ideal setting for the exercise, because a hijacked transport carrying a weaponized cargo could easily cross several jurisdictions, including an international border, and quickly become a threat of national significance. The location amply illustrates the need for effective

*Dale Ferriere is a deputy director at the National Infrastructure Institute’s Center for*



*Infrastructure Expertise, where he supervises all maritime security research projects. He came to NI<sup>2</sup>-CIE after working 12 years in the international maritime transportation industry. Ferriere is a graduate of the U.S. Coast*

*Guard Academy and serves with U.S. Coast Guard Sector Northern New England as Commander, Senior Reserve Officer and was mobilized in support of Hurricane Katrina recovery operations.*

*Payton Garbarino is a project manager at the National Infrastructure Institute’s Center for*



*Infrastructure Expertise, where he’s currently involved in the Canada/United States Cargo Security Project and the School Multi-Hazard Assessment & Resource Tool project. Garbarino has a bachelor’s in criminal justice and a master’s in*

*national security and public safety.*

multi-agency response interoperability: effective command, control, communications and computer-links between local, state and federal responders.

The exercise included a participant playing the role, in real time, of a transport company's logistics manager. Using the geo-fencing application of the chosen tracking device, the logistics manager can monitor a cargo container's geographical location. Both tests simulated a container loaded with a hazardous cargo that could easily be converted into a weapon.

The container's notional port of entry into the United States was the P&O marine terminal at the port of Portland, Maine, and its destination was a warehouse in Bangor, Maine. Since the transport's primary route was north on Interstate 95, a geo-fence was established about the I-95 corridor from Portland to Bangor.

If the transport were to unexpectedly depart I-95 north, an alarm would be sent to the logistics manager. Being fully aware of the container's planned destination, route, departure time and estimated arrival time, he would know that the transport driver should have had no reason to depart I-95.

Without warning, the transport broke its geo-fence near Augusta, Maine. This was the catalyst for the GPS monitoring device to alert the logistics manager. Using a secure Web site and electronic map, he quickly identified when and where the hazmat container had deviated from its intended route.

Unable to contact the driver by cell phone, the logistics manager quickly determined that a hijacking had occurred. By then, the electronic tracking system showed the vehicle moving south on I-95, across the Maine/New Hampshire border and then across the New Hampshire/Massachusetts border. This raised urgent concern that Boston's financial or historic districts could be targets of a terrorist attack.

### Interagency notification

During the initial test, the logistics manager notified law enforcement and first responders by using a pre-established Web link with the New England

State Police Information Network, a regional component of the Justice Department's Regional Information Sharing System network.

Although not structured to deal with emergency situations, the Web link between the "transport company" and NESPIN proved to be very capable at alerting law enforcement and responders from all levels of govern-

ment about a potential container-based terrorist incident.

For instance, after the incident information was transmitted to the NESPIN site, the former director of homeland security for New Hampshire (playing the role of a state official) acknowledged receipt of the incident information by e-mail and simulated taking immediate action. This demonstrated

## Training Exercises

that officials from other law enforcement agencies (local, state and federal) could have been effectively alerted.

For the second test a week later, the logistics manager contacted the U.S. National Response Center <www.nrc.uscg.mil> by telephone and e-mail. The NRC watch-stander quickly documented the incident and sent alerts to federal and state agencies. A follow-up phone call from the NRC watch-stander to the logistics manager verified that these notifications were successful. The NRC proved to be very proficient at initiating a multi-jurisdictional response, especially at the federal level.

In addition, to avoid falsely alarming a state emergency 911 public safety answering point, NI<sup>2</sup>-CIE conducted a pre-exercise visit to the PSAP and interviewed a watch supervisor.

### Lessons learned

**Communications and notification:** Although NESPIN, NRC and 911 PSAP emergency notification protocols demonstrated an adequate ability to initiate a response to a potential terrorist attack involving an intermodal container, some limitations were identified in the overall response system's ability to pre-empt such an attack.

NESPIN and other RISS networks are not uniformly recognized by some of the federal agencies that would have juris-

## Transport industry's plans not up to speed

To better understand the transport industry's emergency notification and response capabilities, NI<sup>2</sup>-CIE interviewed several Canadian and American transport operators as part of this project.

With respect to the exercise scenario described in this article, these companies were asked about their abilities to initiate an effective response based on their emergency preparedness plans. The transport company managers were also asked whether their companies were using, or considering using, commercially available tracking and related technologies, such as smart containers, smart transport vehicles, geofencing and remote shut-off devices on prime movers.

It was found that most transport companies do not have effective multi-jurisdiction emergency response protocols in Canada or the United States. Most of their emergency plans simply rely on emergency 911 for initiating a response. Several companies were unaware of the U.S. National Response Center and its capabilities, and many were similarly unaware of the U.S. National Response Plan. Transport company managers freely admitted, however, that a top-down approach as provided by the NRC would be extremely beneficial for reporting a potential hijacked tractor-trailer, especially when an incident involves more than one state.

Lastly, research showed that very few transport companies would voluntarily invest in an enhanced supply-chain tracking technology unless they were mandated to do so by regulation.

