Closing the Holes in the Air Cargo Security Net

ALPA hosts an eye-opening course on how to deal with threats to the security of air cargo.

Not a secret: Some of the holes in the air cargo security "net" are—well, big enough to drive a truck through.

In early November 2006, ALPA's President's Committee for Cargo, with support from the ALPA National Security Committee, hosted a 2-day, by-invitation-only, Air Cargo Risk Assessment Training Program at the Association's Herndon, Va., building. Attending the training were MEC security coordinators from ALPA pilot groups in the United States and Canada, and representatives from cargo airline managements, the U.S. Department of Homeland Security and Transportation Security Administration, Transport Canada, and other groups with a stake in air cargo security.

Teaching the course was an expert—Amotz Brandes, director and managing partner of Chameleon Associates LLC, a California-based security consulting firm.

"When I worked for El Al, we conducted risk assessment on every single shipment," Brandes declared. "You cannot duplicate the system El Al uses—but you can adopt the principles." Before getting to those principles, Brandes said, the first day of the class would be not about security, but on "how to be a terrorist. Because first, you have to know how to blow stuff up."

The threat

Modern terrorism is indiscriminate, politically motivated, and driven by news media exposure, and focuses on "soft" targets —i.e., the public and the economy. State-sponsored terrorism is a formidable challenge, because it involves essentially unlimited funds, the ability to assume legitimate identities, and the ability to train in a safe environment and work under diplomatic cover, and provides accessibility to means of aggression.

Terrorism usually involves 1–5 years of careful planning, with terrorists taking the time necessary to learn security loopholes and the operational environment of the target, and rehearsing the plan through dry runs.

All terrorist plots, Brandes claimed, involve eight steps: marking (i.e., determining the time, date, location, symbolic value, and physical features of the target), gathering intelligence, surveillance, planning, tooling up, training/rehearsing, execution, and getaway. "Our focus," he said, "is on execution, where it is normally too late—our efforts should include the attack's preliminary phases, which usually take years to accomplish."

The potential means of aggression are several—chemical, biological, radiological, nuclear, sabotage, and explosive—the latter being available, easy to handle, controllable, and easy to test (vs. the other four), Brandes explained.

Though cargo presents unique opportunities to terrorists, it also presents difficulties, including "so many delays with cargo," Brandes pointed out. "Also, the potential fatalities from attacking cargo are not as many as with passenger airliners. And the shipment may end up being shipped by land."

Limitations of security technology

Current security screening technology is not now, and may never be, perfect. X-ray machines can detect some, but not all forbidden items, and CTX machines are being used only with passenger operations.

Certain substances, like glycerin, used in many hand creams, can create false positives when subjected to screening by devices used to detect traces of explosives. False positives occur, Brandes said, "when the system classifies an action as a possible intrusion when it is actually a legitimate action. A false positive is a conclusion drawn without an investigation or questioning. A suspicion, by contrast, involves a conclusion resulting from an investigation or questioning."

Metal detectors can be effective in screening nonmetallic shipments—e.g., fish and produce.

All this bomb detection technology notwithstanding, Brandes asserted, "If I was in a decision-making position in the TSA, the first thing I would do is start using bomb-sniffing dogs, and publicize it. In Israel, we use bomb-sniffing dogs a lot now in mass transportation. This greatly reduces opportunity for terrorists."

The security process, Brandes said, involves three "D's"—

JAN W. STEENBLIK

Israeli security expert Amotz Brandes shares his cargo security expertise with attendees of the Air Cargo Risk Assessment Training Program, sponsored by the ALPA President's Committee for Cargo with support from the ALPA National Security Committee.

Profiling that Works

Brandes pointed out the ultimate futility of attempting to profile terrorists by gender, age, or race. The first terrorist to attack Tel Aviv's Ben Gurion International Airport (in 1972), he said, was a Japanese citizen—because the Japanese Red Army made a deal with the Palestine Liberation Organization to conduct attacks in each other's countries to bypass security forces looking for locals or those who fit the racial profile.

Predictive profiling, Brandes advised, is "a method of situational and behavioral assessment designed to predict and categorize the potential for inappropriate, harmful, criminal, and/or terrorist behavior." He stressed, "You never profile people, objects, or situations. You're profiling an AMO. Don't confuse an AMO with a scenario. An AMO represents a proven, actionable terrorist method. A scenario is an outline or model of an expected or supposed sequence of events. You prove a scenario by using AMOs."

Brandes defined a "suspicion indicator (SI)" as "an indication based on known (or predicted) terrorist or criminal methods of operations or deviation from a typical profile that may lead one to believe that an observed situation (persons and/or objects) may have the potential for harming the protected environment and its inhabitants."

Threat, he added, is "suspicion that was not refuted." Moreover, "threat is constant, while risk is a variable. You have to understand terrorism on the operational level—the threat—before you can assess risk."

The first steps toward predictive profiling are to define

- the protected environment,
- the operational environment (to define all possible AMOs),
- the terrorists' capabilities,
- one's own capabilities and resources,
- the calculated risk, and
- the security objective.

Of these, said Brandes, the latter task is "the most important thing you will do."

He explained El Al's cargo profiling technique, which, for security reasons, cannot be described here. As a general principle, Brandes offered this observation: "In cargo profiling, the best tool for terrorist threat mitigation and prevention is questioning or inquiry."—*JWS*

(1) detect suspicion, (2) determine an aggressor's method of operation (AMO), and (3) deploy against the AMO.

"Detect is the easiest thing we can do," Brandes explained. "Determining the AMO and deploying against it are what El Al is so good at—and which is what the rest of the world needs to learn. If you can't do this, you can't do security."

Technology and humans together are important for the detection step, but "determine" and "deploy," said Brandes, "will always remain human processes."

A never-ending cycle

Brandes put it all together in what he calls "the cyclical security engineering process," which has five parts:

- Red teaming—i.e., testing your own system, based on "marking to getaway"—tests all possible AMOs. "The *first* red-teaming exercise you conduct is *not* to prove a point," Brandes emphasized. "It's to define the AMOs."
- Assessment focuses on the potential for new and existing AMOs to be successful, and the ability of one's own personnel to "detect, determine, and deploy." Assessment involves examining the configuration of technology and security systems, plus policy and procedures, in mitigating the threat.
- SOP design involves articulating new AMOs and suspicion indicators, and writing new procedures for everyone involved in cargo security—including sales and marketing!
- Protocol integration has to do with building a decision-making matrix and integrating new technologies, systems, and procedures.
- Training is based on SOPs. On-the-job training is very important in complex cargo operations. Awareness training—i.e., not security training, but terrorism training—is vitally important.

Brandes said, "I can't stress enough the importance of red teaming."

The first of the six steps in the red-teaming process is establishing the objectives. Step two, tooling up for the exercise, involves gathering props, developing the red team "cell" (which may include persons outside the company), and creating "the overarching story behind the test." The next step is coordination and supervision.

Debriefing after the exercise, the fourth step in red-teaming, should involve the entire staff.

Assessment of the exercise is the next step. Brandes stressed the importance of informing the entire security force about the successes and failures of the exercise.

The last step, involving security personnel in the assessment process and using their operational input, is important, Brandes said. Doing so creates accountability and responsibility among members of the security force.

One TSA aviation security inspector for cargo who attended the course said later, "The training was great and the discussions were excellent. Your members take the threat against air cargo very seriously. You are supporting DHS and TSA efforts to partner with industry for a layered security system."

The training program concluded on a high note, clearly having stimulated the attendees, including representatives of various government agencies. The ALPA President's Committee for Cargo and ALPA's National Security Committee will remain engaged with them in an effort to include air cargo risk assessment methodologies in the system for securing air cargo.—*Jan W. Steenblik, Technical Editor*