

Homeland Security Forces Seek Help from Optical Science

U.S. Customs and Border Protection use sophisticated X-ray equipment to detect contraband in packages and luggage.

James R. Tourtellotte

Tom Price

Science—especially optical science—shows great promise for helping federal officials to protect Americans against terrorism. In December 2005, OSA held a conference in Washington, D.C., that explored optical solutions to homeland security.

Calling the high technology industry “one of our asymmetrical strengths” in the war against terror, the Defense Department’s Peter Verga said optics “can be a significant force multiplier” in homeland protection.

Many optical devices have already been deployed. Off-the-shelf commercial products don’t always meet homeland security needs, however. And products developed for the Defense Department may have to be redesigned before they can be applied to homeland security.

Homeland security officials’ wish lists can seem grandiose. “I want a little box on every telephone pole in the country that tells us when there’s something bad in the air,” said Verga, the Pentagon’s principal deputy secretary for homeland defense, at the OSA-sponsored meeting. Texas Republican Michael McCaul, of the House Homeland Security Committee, talked of deploying stationary sensors and unmanned aircraft to create a “virtual wall” along U.S. borders.

When converting wish lists into product purchases, these officials are realistic, however. Government budgets are far from unlimited, and homeland security forces have a big country to protect. Holding down costs is a paramount concern, and that’s one reason why expensive military devices often can’t be applied to homeland security.

“The Department of Defense reviews technologies for potential uses in homeland security and makes them available to civil authorities,” Verga said. Night-vision devices are a good example, he pointed out, because “police like to see at night, too.”

State and local governments—and even federal civilian agencies—often can’t pay the high price of military equipment, however. Procurement officials sometimes can cut costs by removing military specifications that aren’t needed in a civilian environment—requirements that a device be hardened for a nuclear battlefield, for instance. And they look for new tech-

nologies that use automation to cut costs while improving performance.

The Biowatch program, intended to warn of the release of biological weapons, illustrates those hopes for technology.

To field the system quickly, the Homeland Security Department added biological weapons detectors to devices that the Environmental Protection Agency already had deployed to test air quality in various locations around the country. Because workers have to retrieve filters from the monitors and take them to a laboratory for testing, the system works too slowly and costs too much.

The department wants a fully automated system that could identify hazardous material and report it instantly, said John Vitko Jr., director of the biological countermeasures portfolio in the department’s Science and Technology Directorate. It has to be inexpensive, of course, because it needs to be deployed in a seemingly infinite number of places.

Automation and remote control are recurring themes on those wish lists—and for good reason: When you're trying to deter suicide bombers, for example, you want to locate them without putting those who are doing the detecting at risk. Moreover, a nation the size of the United States can't afford to place a person at every surveillance point.

Bomb-detecting systems that are deployed now are "close-in, slow and of very high risk to screeners," said Roshni Sherbondy, who heads the S&T Directorate's explosives portfolio. A suicide terrorist at an airport check-point can kill a large number of people by setting off his bomb even after he's been detected, for example.

"The bottom line is we want to detect the (bomber) en route to the target," she said. "The goal is to put the detection out as far as possible."

Another goal is to avoid mistakes. A terrorist has to evade detection only once to succeed, while defenders fail if they don't catch would-be attackers every time. Thus, surveillance devices with high sensitivity are critical.

However, it's important to realize that false positives can be nearly as damaging as false negatives. Commerce would be crippled and individuals inconvenienced if erroneous sensing of threats caused transportation systems, office buildings, retail centers and other public facilities to be shut down or evacuated. Frequent false warnings could lead people to ignore the accurate ones.

Desires for speed and privacy also complicate detection. Because of slow security screening procedures, travelers today can spend more time working their way through the airport than they do in flight.

One of the faster and more effective devices for detecting weapons under clothing—a low-dose x-ray machine—reveals the naked body under the clothing as well. While the device is commercially

available, said Barry Smith, a physicist in the Homeland Security Department's transportation laboratory, its use in the United States has been opposed by some who view it as a violation of privacy.

Other countries, he said, do use it, after having established what they consider to be adequate privacy safeguards—employing screeners of the same sex as the passengers being screened, for instance, and stationing the screeners out of eyesight of the passengers.

The United States has been vulnerable for a long time because of its open soci-



Using a highly sophisticated scanner, a CBP officer looks for organic and inorganic materials that could be considered dangerous.

James R. Tourtellotte

ety, vast size and complex transportation and communications infrastructure, said Yacov Haimes, a risk management expert at the University of Virginia. "Nothing changed on 9/11," he said, except for a wider realization of what our vulnerability is.

The threat posed by terrorists does change, however, and that throws another complicated challenge at those charged with securing the homeland.

"We've learned that the terrorists will develop counter-measures to our counter-measures," Sherbondy said. "And we need to counter that."

To do that, Verga said, the defenders and the scientists who support them must always be pursuing new strategies, tactics and devices. "The enemy adapts," he said. "It's going to be a constant battle to stay ahead." ▲

[Tom Price (ThePricesWrite@yahoo.com) is a journalist who focuses on government, politics, technology, business and education.]

80 milliseconds of spectra captured during the warm-up period of an Ocean Optics LS-1 Light Source. The data was collected in raw, unprocessed intensity mode.

Collect 1,000 High-resolution Scans per Second!

Ultra-fast, High-resolution Spectrometer

The HR2000+ generates up to 1,000 full spectral scans every second and can achieve optical resolution to 0.035 nm (FWHM). It's an ideal solution for chemical, biochemical and other applications where fast reactions need to be monitored and fine spectral features need to be resolved.

- Powerful 2-MHz A/D converter for 1 ms integration time
- Resolution to 0.035 nm (FWHM)
- Multiple triggering options
- Responsive from 200-1100 nm, specific range and resolution depends on your grating and entrance slit choices

Just **\$3,499!**

US: 727.733.2447
 Europe: +31 (0) 26 319 0500
 OceanOptics.com
 Info@OceanOptics.com