Seaports, shippers, and the government are linking their efforts to maintain a critical infrastructure.

By John DeGaspari, Associate Editor

he terrorist attacks on New York and Washington on Sept. 11, 2001, shocked everyone, but they conveyed a special message to those charged with protecting United States ports. One of the stated goals of Al Qaeda is the destruction of the U.S. economy, and maritime trade is an economic linchpin. What's more, the 9/11 attacks suddenly exposed modern seaports, with their vast linked transportation and storage infrastructures, as the soft underbelly of security in the country.

Ports have been a security issue since the days of the Revolutionary War, said Victor Zaloom, chair of the industrial engineering department at Lamar University in Beaumont, Texas. He also heads the Center of Ports and Waterways, the university's center for the study of maritime issues. But the focus has changed. Before 9/11, ports were concerned mainly with theft, vandalism, or accidents. Now the worry is about someone doing intentional damage, he said. “It puts a different slant on the whole concept of security and raises the bar significantly,” he said.

Protecting that infrastructure is critically important. Between 1990 and 2003, the value of maritime trade to the U.S. economy ballooned from $434 billion to $800 billion, according to Alan Erera, an assistant professor with the School of Industrial and Systems Engineering at the Georgia Institute of Technology in Atlanta. In one sense, those numbers reflect the country’s growing trade imbalance. They also mean that more high-value cargo is crossing U.S. borders than ever before.

The rising importance of ports, however, presents them with a particular challenge when it comes to tightening their security measures. Over the last few years, ports have struggled to protect their assets without disrupting commerce, which could result in severe economic consequences. According to Erera, “Ports need to be protected because they are so valuable, but they have to be protected carefully because they are so valuable.”

Just as magnetic resonance imaging has become a standard for securing luggage systems at airports, the global positioning system and radio-frequency identification are being enlisted to control ocean-borne shipping containers. However, not everyone
Roger Johnston, a research scientist at the Los Alamos National Laboratory in Los Alamos, N.M., thinks that employing good security requires an understanding of the limits of technology. Johnston heads up the laboratory's Vulnerability Assessment Team, a group that tests intrusion and tamper-detection devices. Over the last 13 years, the group has tested a range of devices, such as security tags, tamper-indicating seals, radio-frequency identification devices, and global positioning systems.

Johnston said that technology plays an essential role in security applications, such as access control, and cargo monitoring, but he warns against having “blind faith” in what technology can accomplish.

He warns against a tendency to confuse devices designed for inventory with those meant for security. Inventory systems often undergo what he terms “mission creep,” in which devices that were originally designed for inventory control over time become viewed as security devices, even when little or no security was designed in, he said.

Although some devices can serve both purposes, they should be evaluated separately for each application, he said. “Analyze the system as a security system and see the pros and cons. Then step back, start over again and analyze it as a security system, rather than lumping them all together.” Johnston also warns that there is not much of a relationship between the expense of a device and its security effectiveness.

RF identification tags are often touted by some officials as security devices, said Johnston, but are not effective security devices. They are easy to lift, counterfeit, and spoof, he said. He said that he is not opposed to using RFID tags, “but we need to think about what they are really doing for security, and at this point they are not doing anything,” he said.

Global positioning system devices have no security built in, but they are being used increasingly for security devices, according to Johnston. GPS receivers tune into a constellation of satellites to determine the location of a vessel. Commercially available satellite simulators can send out false signals that can easily fool many GPS receivers, Johnston said. He said encryption schemes to report the location back to a home office do nothing to increase security if the signals can be faked.

Tamper-indicating seals are used to detect unauthorized access or tampering. They show evidence of tampering after the fact. They must be inspected, either electronically or manually, to determine if unauthorized access has taken place.

Inexpensive mechanical seals may indicate an intrusion by the destruction, damage, or some modification to the seal body. Electronic or electro-optic seals may store an alarm electronically or magnetically within the seal. The problem with this approach is that someone can hide or replace the evidence of tampering or replace the seal with a counterfeit, Johnston said.

According to Johnston, a better approach is to store “anti-evidence” information when the seal is first installed that tampering has not been detected, which is erased when the seal is opened. “There is nothing for the bad guys to hide or repair or counterfeit, because the information is gone,” he said.

His group has developed electronic and even mechanical anti-evidence seals that use this principle. He calls the mechanical version the Magic Slate seal, which uses a dry erase marker. The idea is similar to the children's toy plastic slate, in which the writing is erased when the plastic sheet is peeled back, he said.

He added that anti-evidence seals are fully reusable, even mechanical ones. They also have an “anti-gundecking” attribute. Gundecking, a term borrowed from the Navy, refers to falsifying reports, as in the case of an inspector who may claim to have checked a seal for tampering when in fact he did not. Anti-evidence seals make it possible to check up on a seal inspector by not telling him what the anti-evidence is in advance, he said. He calls this a particularly important advantage over conventional seals in real-world use.

Johnston believes that better seals are possible. But he
also thinks that security can be improved by a little bit of training. "Security is about paying attention," he said. "You have got to have people asking questions and thinking. And you can't just automate this process. It's too easy for bad guys to find loopholes." The bottom line, he said, is that technology is a useful tool, but security is really about people.

**ASSESSING RISK**

There are limits to resources. ABS Consulting, a risk assessment group based in Knoxville, Tenn., has worked with the U.S. Coast Guard in developing port vulnerability analysis and maritime risk management.

According to Myron Casada, vice president for offshore, ports, and terminals for ABS Consulting, probably the biggest focus in port security since 9/11 has been on restricting access and knowing who has access.

Port security is a combination of screening at foreign ports, tracking incoming vessels to U.S. ports, and protecting ports at home with measures that include gates, guards, cameras, and access control.

"It takes a very broad program to address different kinds of concern," Casada said. In deciding where to spend their money, ports must ask themselves what they are trying to accomplish. "We are not going to see a world of zero risk at any level of investment," he added.

David Walker, ABS Consulting's vice president of technology, said there has always been an awareness of sabotage and theft in ports, and that has put them in a good position to begin work on terrorist issues. Yet the challenge of terrorism is largely new, he said.

In terms of risk assessment, the fundamental tools are largely the same. Assessing the risk of randomly occurring events requires looking at frequency and consequence. Security puts a slightly different twist on that. It is viewed in terms of threat, vulnerability, and consequence. Threat is the potential frequency of attack; vulnerability is the likelihood of success if someone tries; and consequence is the damage of an attack—to life, limb, property, the economy, and cultural icons.

According to Walker, the focus of security risk assessment is on long-term as well as initial damage. "When you destroy this asset, you are really impacting the supply chain, which has broader impact for companies and regions of the country," he said. A constant issue for ports is trying to keep the supply chain operating while providing security.

Fred Enoch, a security specialist at ABS Consulting's Houston office, said there has been a big push on better intelligence, through working with foreign ports to detect problems before they approach U.S. shores. The focus of security has changed since 9/11, Enoch said. "In ports, crime has always been a problem and stowaways have always been a problem. But the seriousness of it has changed. The overall security awareness has changed, in having everyone pay more attention, because it may not be a stowaway or a political refugee," he said.

A mobile gamma ray imaging device can be set up quickly, to screen the contents of sealed shipping containers that are in transit.
The Department of Homeland Security speaks of a layered security strategy, in which the U.S. Coast Guard and Customs and Border Protection work with private, state, and local agencies to cooperate on a system of various security measures that are designed to protect three phases of the journey: overseas, in transit, and on U.S. shores. The idea is to push security outward from U.S. borders. Many security initiatives were put in place after 9/11.

For example, most sea carriers must now provide proper substantial container traffic to the United States. Ports working under the program allow U.S. Customs personnel to inspect cargo that originates, moves through, or exits a port. The ports are equipped with non-intrusive equipment, such as gamma ray or X-ray and radiation detection equipment for screening containers. Participating foreign ports also agree to establish an automated risk management system; share critical data, intelligence, and risk management information; conduct a thorough port vulnerability assessment; and maintain integrity programs to identify breaches in security. To date, 19 of the top 20 foreign ports have signed on to the program, accounting for about two-thirds of the container traffic to the United States.

Ships bound for U.S. ports must notify the Coast Guard 96 hours before arrival, and provide detailed information about crew, passengers, cargo, and voyage history. This information is analyzed using databases and intelligence information, to search for evidence of previous security problems with the vessel or illegal activity on the part of the crew.

Each U.S.-bound container is given a risk assessment number, and suspicious ones are flagged on arrival for further investigation, which may include passing through a gamma ray inspection machine. These large-scale imaging systems can scan the interior of 40-foot containers in less than a minute, according to the Department of Homeland Security.

Port personnel are equipped with portable radiation detectors; there are currently several thousand in the field, according to Bill Anthony, a U.S. Customs and Border Protection spokesman. In addition, by the end of this year, most U.S. ports will be equipped with radiation portal monitors to screen cargo entering or leaving the port. The monitors are sophisticated enough to identify the type of radiation that is being emitted.

There are old security hands as well. Port security teams use dogs trained in sniffing out drugs, explosives, and chemicals. Most ports have dogs trained to find drugs and explosives, and are quickly expanding the ranks of chemical-sniffing hounds, Anthony said.—John DeGaspari
Bert Macesker is the program manager for risk assessment tools at the U.S. Coast Guard R&D Center in Groton, Conn. He said that the Coast Guard works with ports in testing new countermeasures. “There are a host of new technologies that we are considering across the board,” he said. The Coast Guard has developed risk assessment tools that are now used in assessing risk by Captains of the Port, the officials who direct Coast Guard law enforcement activities, and by Area Maritime Security Committees, which coordinate activities among law enforcement groups, industry, and the boating public.

Knowing the risks is the first step before deploying security assets, he said. The Coast Guard has a risk assessment model for looking at the dissipation of threat, vulnerability, and consequence, he said. “It gives us a sense of what our priorities are and what we need to protect most in terms of various activities,” he said.

Macesker said that the Coast Guard was already working on risk tools before September 2001, and trying to develop the right tools for prevention and response. Some of the issues were safety, fuel transfer, and passenger vessel inspection. Now many of those logic-modeling tools have become important to security risk analysis, he said. Macesker said, for example, that he is looking at a standard analysis tool for the chemical process industry and is using it to evaluate security barriers.

Risk tools are also being used to evaluate new investment areas for technology, he said. Among them are programs for underwater port security, the use of unmanned aerial vehicles, and automatic identification systems for ships. Risk tools are also being used for consequence modeling to understand how bad attacks can be, he said.

Macesker acknowledges that security is not all about high technology. Sometimes, a well-tailored system of countermeasures can be better than one piece of super-technology, he said. A many-layered approach of even low technology may be more of a deterrent, because complicated technology can be perceived as being unreliable in some security situations, he said. “We need to develop measures of how much deterrent effect technologies provide. And that is a very hard thing to do,” he said.

The attacks of 9/11 forced U.S. ports to confront security in an entirely new light, and in many ways ports are grappling with the best way to handle it. In general, in terms of security regulations development and compliance, progress has been pretty good in that there have not been significant adverse impacts on productivity, said Alan Erera of Georgia Tech.

On the other hand, many people think that ports still have significant vulnerabilities to terrorism. Additional tightening of security may well hurt productivity, Erera said.

Security issues are having an effect on companies that operate on a global scale, he said. Companies have to consider not just how well global supply chains work, but how susceptible they are to disruption. “There is a renewed sense of the fragility,” he said.

It's not all cargo: One million cruise ship passengers are expected to pass through the Port of New Orleans in 2006.