The State of Homeland Security

While observers are sharply divided over how much real progress is being made, the political will and technology now exists -- and that's a huge improvement

On May 12, a simulated explosion in Seattle and the revelation of dangerous germ-warfare toxins in Chicago kicked off a $16 million exercise to test America's first responders and emergency personnel. Thousands of firefighters, police, hospital workers, and others from dozens of federal, state, and local agencies took part. Going under the code name TOPOFF2, the exercise was the largest of its kind to date. Officials hope lessons learned from the event will help all levels of government better understand how to deflect a terrorist attack using weapons of mass destruction.

Announced a week before it took place, TOPOFF2 has become a magnet for both criticism and praise of the vast efforts to shore up homeland security. The glass-half-empty crowd wondered why first responders were told well in advance not only that an exercise would occur but also about the nature of the danger they would face and even the precise location of the different parts of the exercise. The glass-half-full crowd noted that these types of government drills, which have rarely occurred in the past, are becoming a routine part of running the country.

The juxtaposition of those viewpoints reflects the state of homeland security some 18 months after the September 11, 2001, terrorist attacks on New York and Washington: The U.S. is somewhat safer than it was in those innocent days, but the quest for true security has only just begun.

LITTLE LEFT UNTOUCHED. The search for greater security certainly has had long tentacles. At some level it has reached into every nook and cranny of the U.S. Homeland security efforts have touched small-town water systems and big-time telecom companiess, chemical plants in New Jersey, and nuclear reactors in North Carolina. This reaction to the World Trade Center attacks has also engendered the largest modern-era federal reorganization, a massive consolidation of various functions previously conducted by 169,000 employees in 22 separate federal agencies representing $37 billion in government funding into the newly formed Homeland Security Dept. headed by former Pennsylvania Governor Tom Ridge.

The push to shore up homeland security has spurred a dizzying array of research efforts into bioterrorism, chemical weapons, and transportation security, among others. Across broad industries, companies have added guards with guns and have plotted survival strategies in case of physical attack. Many companies have chosen to more widely disperse their employees to prevent the type of catastrophic business interruption Wall Street suffered after the Twin Towers fell.

And yet the questions remain: Is America safer now than before? And if so, has the improvement been commensurate with the level of effort and expenditures so far -- including the U.S. invasion of Iraq? To a large degree, the answers depend in part on whom you talk to. Witness the diverging views of two expert observers -- Kathleen Sarten and Steve Flynn.

SAFER PORT. Sarten is the Seattle service port director for the Customs & Border Protection (CBP) bureau of the Homeland Security Dept. Her job prior to 9/11 was to chase narcotics traffickers, counterfitters, and software pirates who exploit the 100,000 or so tractor-trailer size shipping containers that pass through the Port of Seattle each month. Now, Sarten's job is all terrorism, all the time -- "anything connected with anti-terrorism," she says.

She sees Seattle as a far safer port today. Within the past year, Sarten say she has gotten enough funding -- she won't say how much -- to double the number of staff dedicated to seaport cargo processing and maritime security over the last year. Seattle has also received its own VACIS (Vehicle & Cargo Inspection System), one of 20 such devices ordered by U.S. Customs

since September 11. This truck-mounted machine uses gamma rays to peer inside containers to help customs inspectors spot anomalies that might indicate dangerous cargo. A complete scan of a 40-foot container using a VACIS machine takes less than a minute.

As a result, Sarten's forces can scan suspect containers rather than having to fully unload and manually search them. And today, all of Sarten's inspectors have personal radioactivity-detection badges -- portable Geiger counters that until recently only a few U.S. Customs officials had.

SOUNDS GOOD, UNTIL... New procedures have also helped Customs do its jobs more efficiently. As of March, 2003, ships arriving at the Port of Seattle must forward an electronic list of their cargo to customs inspectors no less than 24 hours before loading up their cargo at a foreign port. And a collaborative program with other governments allows U.S. Customs inspectors to examine loads coming in from foreign ports before the ships even set sail.

Also in the works is a new program called Operation Safe Commerce, a cooperative effort between Customs inspectors and large shippers to computerize and automate the tracking of containers throughout a company's supply chain. The ports of Seattle and Tacoma have requested $36.5 million for the project from the Transportation Safety Administration and have lined up 18 private-sector participants.

All of which sounds encouraging until you speak with Steve Flynn, a senior fellow at the Council on Foreign Relations and former U.S. Coast Guard officer. Flynn remains far less sanguine about the prospect of protecting U.S. ports. While he appreciates the type of progress that Sarten claims, "most of what you have to date are unfunded mandates on the transportation industry," says Flynn. As for the government enforcement agencies, "you have very serious constraints on manpower, [info-tech] backbone, and things you need to maintain a serious presence."

OUTDATED SHIPS. He also thinks Washington has been too parsimonious. While some money has been forthcoming, to date Congress and the Bush Administration haven't shown a huge interest in spending big bucks for transportation security, says Flynn. He points to a $1 billion bill floated by North Carolina Democratic Senator Fritz Hollings that lost by six votes. In the current Homeland Security budget, Flynn feels the increases have mainly covered ongoing operational costs and manpower with very little going toward capital improvements.

Take the U.S. Coast Guard. The White House significantly raised its budget to $3.5 billion in fiscal 2003. That included a $650 million request to upgrade the USCG's deepwater capabilities. However, Flynn points out that the Administration has stuck to a 30-year replacement cycle for the majority of the Coast Guard fleet. That means for the foreseeable future its seaborne interdiction capability will depend of outdated ships running older technology. In fact, observers are still trying to pick through the budget requests and the big consolidation at Homeland Security to discern whether some functions will actually receive less funding in 2004 than in 2003.

What also bothers Flynn is that some of the technology that could make it far easier for the U.S. to track ships is easily affordable. Equipping the 40,000 or so seagoing cargo vessels of significant size with a satellite beacon that would allow the U.S. or anyone else to track them anywhere on the globe would cost $1,500 per ship, he says. The total cost of equipping the world's fleet with the means to create a global seaborne traffic-control system would run less than $60 million in up-front costs with minimal upkeep. "That's chump change," says Flynn, who notes such a system could easily be international in nature and might improve safety for the global shipping trade.

REPEATING PATTERN. No doubt, it's easy to take either side of the argument, and both are correct in many respects. People inside the government often express a "can-do" attitude sorely lacking in the past. But at the same time detractors like Flynn question whether the priorities are correct, the progress is real, and the entire effort isn't paper-thin.

This pattern of raging optimism and gnawing skepticism appears across the homeland security spectrum. In matters of chemical-plant and storage security, critics claim that the chemical industry has resisted serious efforts to enforce more stringent security measures to safeguard the 15,000 facilities that hold what the Environmental Protection Agency considers to be dangerous substances. But EPA homeland security liason Robert Bostock points to legislation moving through Congress that would allow the EPA to levy $250,000 fines against plants that fail to meet safety standards.

Critics of the nuclear industry say the Nuclear Regulatory Commission has failed to adequately police the sector, allowing lax security and avoiding any serious enforcement actions. But Roy Zimmerman, NRC deputy director of nuclear regulatory research, says his agency is about to resume more stringent security-testing drills, also known as "force-on-force" drills, which pit inspection teams against plant guards in simulated combat designed to mimic terrorist assaults.

MIXED REVIEWS. The NRC is also in the process of updating its evaluations on how susceptible various plant structures are to airborne attacks or explosive devices. That's thanks to additional funding of $30 million, money the NRC could never have received in the pre 9/11 environment.

When it comes to the private sector, the reports are generally mixed. Telecoms have won accolades for sitting down together on the Network Reliability & Interoperability Council to lay out joint plans for weathering a terrorist attack. And many key infrastructure providers in the power, water, and utility sectors have put in place more guards, guns, and physical barriers to ward off attackers seeking low-hanging fruit.

At the same time, critics wonder why the airline industry, the recipient of so much federal largesse, refuses to match bags to individual passengers on domestic flights. This practice is mandatory in Europe and is considered by experts to be a key security provision.

And Flynn wonders why companies shipping goods across the globe at rates less than half what they were five years ago would resist small price increases levied by transportation companies. "To increase the cost of shipping on a $120 pair of Nike's from 30 cents to 50 cents is not going to upset the free-market system," he says.

PRIVACY CONCERNS. Increasingly, though, homeland security initiatives have run afoul of civil libertarians. Screening procedures for immigration processes and air-travel passengers that involve deep background checks against large databases and, in the case of immigration, biometric identification, have raised particular ire. Critics say the powerful new databases add little to security since the authorities could easily have tracked the 9/11 terrorists with existing means but failed to do so for because of a stifling bureaucracy and poor police work.

"Efforts by federal agencies to incorporate computerized travel records into government dossiers have created an urgent need for comprehensive federal travel-data privacy legislation modeled on the data-privacy laws in Canada and Europe," says Edward Hasbrouck, author of a travel book series titled The Practical Nomad and a vocal critic of the Transportation Safety Administration's new iteration of the Computer Assisted Passenger Screening System, dubbed CAPPS II (see BW Online, 3/27/03, "Putting the Blinders Back on Big Brother"). Congress so far has expressed its own misgivings with the current balance between security and privacy by refusing to pass a new, more intrusive version of the U.S. Patriot Act, key parts of which are scheduled to expire in 2005.

Meantime, the hype over the ability of technology to improve homeland security continues to outrun its achievements. Most projects using truly advanced technology remain in the pilot phase -- even though they offer insights into a new era when much of the drudge work that now depends on humans -- and that suffers from human error -- will be automated. At North Island Naval Air Station in San Diego, the military has installed a computer-driven system from Atlanta

company VistaScape that uses data culled from images grabbed by high-quality video cameras to create a virtual visual perimeter around ships.

JUST THE BEGINNING. This could ultimately replace sailors with binoculars scanning the horizon. Designed to prevent a repeat of the USS Cole attack where a small boat laden with explosives blew a hole in the side of a Navy destroyer anchored in Yemen, the VistaScape system can spot small craft as far as 4 kilometers out and relay their exact coordinates to officers on watch. "The software doesn't blink," claims Glenn McGonnigle, VistaScape's CEO.

Both critics and boosters of homeland security efforts to date agree that the journey toward better security is just beginning. Seattle's Sarten recalls a conversation she had recently with a Chinese shipping official. He explained that in many parts of the Middle Kingdom, the first stage of logistics involves bringing products to a small truck on a horse-drawn cart. That small truck is driven to meet a small train. The small train is then moved to meet a larger train carrying standard containers that, finally, make it onto the ship.

Sarten's point? Even if U.S. inspectors look at the final step of the delivery process, they'll miss the previous four. "You can put a good seal on a bad cargo, and all that means is that you have put a good seal on something you don't want to allow into the U.S., anyway," she says.

SIMPLE STEPS. In other words, basic intelligence and legwork still remain the key factors driving enhanced security. "What has worked well is good old-fashioned police work. Investigating terrorist networks has resulted in arrests. Interdicting terrorist funding has worked. Rolling up terrorist networks, both at home and abroad, has made us all safe," says Bruce Schneier, a security expert and publisher of the Crypto-Gram cyber-security newsletter.

In that respect, despite big failings and perhaps a lack of vision, the Bush Administration has enhanced safety by boosting security staffing and taking basic but previously overlooked steps to ensure better coordination among agencies and between the private and public sectors. The TOPOFF2 exercise running the week of May 12 is an example of that. Sure, it's a bit of a cakewalk. But it'll help get homeland security responders and planners ready for more rigorous tests later. After all, getting in the right frame of mind is half the security battle.

Disponível em: <http://www.businessweek.com>. Acesso em: 10 jun. 2003.