From:
http://issues.org/18-2/bonvillian/
Fall 2002

Homeland Security Technology

by Kendra V. Sharp, William B. Bonvillian

A new federal agency is needed to rapidly develop and deploy technologies that will limit our vulnerability to terrorism.

On September 11th, our complex national aviation infrastructure became a brilliant weapons delivery system, both stealthy and asymmetrical. The attack was so successful that we should expect this and other like-minded groups to strike again at our homeland. The nation has rallied to improve security at airports, public buildings, and other likely targets. But these efforts have made painfully clear how vulnerable the country is to attackers willing to kill not only innocent civilians but themselves as well. Much must be done in all areas of homeland security before Americans feel safe again. Technology will have to play a critical role. Indeed, technology will be every bit as important in ensuring homeland security as it has been historically in creating military dominance for the armed services. Of course, technology has already been enlisted in areas such as airport security, and technology exists that

can be applied to homeland protection. But much work could be done to find additional ways in which existing technology could enhance security and to do the research needed to develop new technology to meet security needs. The United States has no organization or system in place to fund and coordinate this technology development effort, and we cannot expect the effort to organize itself. We need to evaluate carefully what our homeland security needs are, think creatively about how technology can help meet those needs, and put in place a federal entity with the wherewithal to marshal and direct the resources necessary. A survey of the most obvious areas of national vulnerability demonstrates the profound need for accelerated technology development and deployment.

Aviation security. The World Trade Center and Pentagon attacks illustrated the insecurity of the nation's commercial aviation infrastructure. The insecurity turns out to be even worse than the attacks illustrated. For example, in 1998 and 1999, test teams from the Department of Transportation's Inspector General gained unauthorized and uninspected access to secure areas in eight major airports in 68 percent of attempts and boarded aircraft 117 times. Even after the terrorist attacks, the Inspector General testified that fewer than 10 percent of checked bags were being screened for explosives before being loaded onto the aircraft.
Technology needs to be swiftly implemented and deployed for a comprehensive new screening system for detecting weapons and explosives on passengers and in their carry-on and checked baggage. Advanced surveillance systems are needed to prevent unauthorized access to secure areas, and advanced screening and tracking technology is needed to monitor everything loaded onto a commercial aircraft, including cargo and catering. In the past two months, opt-in "trusted passenger" systems, using biometrics for positive passenger identification, have been proposed for frequent travelers willing to provide personal information in return for faster check-in. Other technology-based options under discussion

are real-time streaming video surveillance of cabin and cockpit transmitted to ground locations, installation of auto-landing systems on compromised aircraft, and biometrics for positive identification of all passengers. Many of the proposed technologies are either already used on a limited basis or could be commercially available in a relatively short time.

The Federal Aviation Administration maintains an R&D program for new technologies, but this must be augmented and accelerated. Critical new technology needs include much faster baggage-screening devices with much better imaging; computer systems that "read" and identify screened images; machines that search for a wider range of contraband; cheaper baggage-screening machines for smaller or mid-sized airports; and passenger-screening machines that can detect nonmetal weapons, explosives, and components of weapons of mass destruction.

Port security. The state of U.S. border control is as disturbing as the pre-9/11 aviation security scenario. In 2000, almost half a billion people, 11.5 million trucks, and 2.2 million rail cars crossed U.S. land borders, and security is being increased at these crossings. But the nation's ports need special attention. Although numerous U.S. ports receive a steady stream of ships from throughout the world and are essential to the nation's participation in global markets, there are no federal standards or no single federal agency addressing the security of our shipping system. More than 200,000 vessels and 11.6 million shipping containers passed through U.S. ports during 2000. Fewer than one percent of containers are physically inspected. The shipping traffic simply overwhelms the current inspection system, which suffers from a lack of resources, poor coordination and communication between agencies, and inadequate inspection technology.

Port and shipping security belong at the top of the threat list for terrorism. Containers are an ideal delivery system for weapons of mass destruction, particularly chemical weapons or dirty nuclear bombs. With the use of a global positioning system (GPS)

transponder, someone could remotely detonate an explosive at any location, making it almost impossible to identify the responsible party.

In recent Senate testimony, Cmdr. Stephen Flynn of the Coast Guard and the Council on Foreign Relations outlined elements of a potential systemic solution for the shipping part of this problem, which relies heavily on technology. He proposed "pushing out the borders" by locating Customs and Coast Guard officials and technology offshore, particularly in the world's megacontainer ports. His proposal includes systems to prevent unauthorized access to loading docks, camera surveillance of loading areas, advanced and high-speed cargo and vehicle scanners, theft-resistant mechanical seals, continuous real-time monitoring and tracking of containers and vehicles in transit by GPS transponders and electronic tags, and electronic sensors to prevent unauthorized opening of containers in transit. Containers that meet advanced security requirements would travel on a fast track to ensure high-speed transport. A number of the technologies proposed are information- rather than hardware-intensive, making them less expensive. In addition to improving security, a more effective tracking system could help combat the industry's serious theft problems, which would enhance its appeal to the shipping industry. Many of these technologies are either currently commercially available or are in the final stages of being evaluated and could be deployed within a matter of months if funding were available. The system as a whole needs to be carefully integrated, tested, and evaluated. Over the long term, there is a need for accelerated R&D on integrated technology for affordable rapid screening of large containers for a wide range of contraband and on technology for rapid dissemination of tracking and intelligence information.

The technology entity will need its own R&D budget to augment existing federal and private efforts as well as to fund new projects.

Bioterrorism. Although numerous researchers and studies warned of the possibility of bioterrorism, the threat had not penetrated the

public consciousness until the October anthrax attacks. Although we've already seen several fatalities, widespread public concern, and major disruptions to the postal system, experts continue to warn that future bioattacks could be far worse. In June 2001, the Johns Hopkins Center for Civilian Biodefense Studies simulated a complex smallpox biowarfare scenario. In this "Dark Winter" simulation, 16,000 people in the United States would have contracted smallpox within two weeks, and smallpox vaccine supplies would have been depleted. The simulation projected that within two months, one million people worldwide would have died. Although we have a vaccine for smallpox, we still do not have any effective treatment. And anthrax and smallpox are only the tip of the iceberg. A hundred other toxins and agents can be weaponized, and we have either very limited or no effective treatment for nearly all of them. Potential genetic modifications of these biological threats multiply the danger.

Remedies for most of the anticipated bioterror weapons do not exist, which presents special development problems. The biotech and pharmaceutical sectors are central to the innovation system in the medical field but have zero market incentive to develop effective vaccines or treatments for bioterror threats, because these products would have a market only in the face of a national disaster. Incentives such as patent, tax, and funding benefits will be necessary to enlist this industry in the battle against bioterrorism. Advance government agreements to purchase and stockpile remedies when developed may help.

In addition to participating in this major R&D effort, the U.S. scientific and medical enterprise needs to reorganize to advise on the management of an attack. To prevent or respond to both known and as yet unanticipated bioterrorism threats, they will need to set care priorities, allocate resources, and establish response protocols.

Cybersecurity. Broadly defined, a secure information infrastructure underlies many of the systems described in previous sections, as well as many of our financial systems, communications networks,

and transportation and other critical infrastructure. In a typical denial-of- service attack against its Internet server in March 2000, a New York firm estimated that it lost $3.5 million in business because its customers were unable to conduct trading. But according to some experts, the mode of attack may be changing from active (distributed denial-of-service) attacks to “passive control,” in which an attacker takes control of certain critical infrastructure elements (including computers or networks) and manipulates them at will. The information technology sector has expanded rapidly without paying adequate attention to information security. Viruses or worms including Melissa, I Love You, Code Red, SirCam, and most recently, W32/Goner have spread with breathtaking speed across the globe. For example, Code Red infected more then 350,0000 computers in less than 14 hours. Although it is difficult to even briefly describe the breadth of current information infrastructure vulnerabilities, the pervasiveness of information technology in all of our critical infrastructure and economic systems demands that information security be a national priority in coming years. Information infrastructure protection and information assurance require increased interagency coordination for prevention, response, and recovery from active or passive attacks; increased commitment to the education and training of information security specialists; an active movement by industry to minimize vulnerabilities through anticipatory rather than simply reactive strategies; and a commitment of governmental and private resources to implement existing strategies for securing their information infrastructure. Although the challenges for deployment of existing technology are daunting, the R&D needs are even greater. We need an aggressive information security R&D effort in new technology approaches such as self-healing networks, sophisticated access controls, and sensor and warning systems.

A model for action

The federal government has played a critical role in defense R&D,

and the homeland security technology needs outlined above require extensive federal involvement. The task crosses many federal agency jurisdictions and falls outside of or in secondary status to established missions, creating a requirement for cross-agency technology coordination, deployment, and development. Although the White House Office of Science and Technology Policy has been effective in coordinating some interagency science and technology (S&T) programs, the scale of the homeland security technology task would dwarf its limited capabilities and staffing. Besides, what is needed here is not just coordination but active technology development and deployment. It is hard to imagine how this can be accomplished without the creation of a new institution, and not just any institution will be up to the job. We need to ensure that the entity created is well suited to the task. War spurred the creation of most U.S. government science agencies, and most of these integrate applied R&D in support of agency missions with elements of fundamental science to allow access to breakthrough opportunities. These integrated agencies, which focus on long-term technology development and employ sizable bureaucracies, do not appear to be lean or flexible enough for the current emergency. In 1958, President Eisenhower faced a similar problem and introduced a different model. Shocked by the Russian launch of Sputnik and determined to avoid another technological surprise, he created the Advanced Research Projects Agency [ARPA, later renamed the Defense Advanced Research Projects Agency (DARPA)]. Designed to spur rapid development of revolutionary technologies, the DARPA culture features talented, highly independent program managers with great budget discretion, flexible contracting and hiring rules, and a skeleton staff. DARPA identifies a technological need, and then the staff contracts with whatever federal agency, university, or company has the capability to meet that need. Once described as “75 geniuses connected by a travel agent,” DARPA has been one of the most successful technology development agencies in history, with the Internet as only one of its innovations. Because of its flexibility and speed,

DARPA serves as a model for a federal program to address the technology needs of homeland security.

One DARPA effort is particularly instructive. In 1992, when the confluence of an economic recession and the end of the Cold War led to a reduction in funding for defense R&D, DARPA was called on to run a Technology Reinvestment Project (TRP) aimed at stimulating development of commercial technology that would also be useful to the military. DARPA received more than $1 billion over three years, enough money to entice other technology development agencies to its table. DARPA spearheaded a true interagency effort, using its funding to leverage other agency investments. The interagency group traveled around the country making face-to-face presentations about its program to private- and public-sector technologists. It succeeded in quickly setting in motion a number of industry-led targeted technology development projects in areas such as rechargeable lithium ion batteries and manufacturing techniques for display screens. The program was unpopular with many military officials who prefer defense-only technology, and it was cancelled when economic recovery eliminated the rationale that it was needed as an economic stimulus. Nevertheless, experience with TRP can be helpful in developing a quick-footed R&D response to homeland security needs.

A DARPA for homeland security

To survive in the Darwinian federal bureaucracy, the homeland security technology entity must be housed in a strong overall homeland security agency with a strong director. The homeland agency director's power will be determined by whether the agency has a significant budget of its own to hire a staff and implement policy; whether it has the ability to review and revise budgets of other mission agencies active in the field; whether it has controls over how those budgets are implemented; and whether it has the authority to set overall missions and compel cooperation among competing agencies. Just as DARPA, at least in theory, has the

secretary of defense as a bureaucratic champion, the technology entity will need a homeland agency director with significant bureaucratic leverage. This authority must be formalized in legislation. Power based only on presidential intervention, which is all that the homeland defense office has for now, is of limited value because no president has the time to participate in all the battles for influence. Because many other mission agencies are already engaged in work that is critical to homeland security, the new technology entity must itself have the ability to ensure R&D cooperation among the existing agencies. Marshalling and coordinating R&D in already-existing programs is the quickest and most effective way to get the job done. The technology entity can succeed without establishing its own S&T bureaucracy, but there are number of powers and characteristics that will be essential to its work.

Its own pot sweetener. Just as DARPA's TRP shared its funding to quickly bring other technology agencies into a truly cooperative relationship, the homeland technology entity will need its own R&D budget that can be used as a pot sweetener. This fund can be used to augment and accelerate targeted existing R&D efforts in federal agencies or private companies as well as to fund new projects. Technology entity project managers should have the flexibility to distribute funds to create cooperative partnership programs among universities, public-sector agencies and labs, and private companies, leveraging private funds with public wherever appropriate.
The aim is not to build a new bureaucracy but to find technology leaders who can deploy existing lab and S&T resources quickly and flexibly.

Lean and talented. The homeland technology entity should follow DARPA's model of hiring outstanding talent in small numbers as project managers in key threat response areas and arming them with funding to make new development happen. The

overwhelming public support for the fight against terrorism suggests that first-rate scientists and engineers would be willing to work for this entity in this time of crisis. The aim is not to build a new lab and a new staff-heavy science bureaucracy; it is to find technology leaders who can deploy existing lab and S&T resources to meet the new need. Glacial civil service hiring procedures and the inability to pull in private-sector employees on specific projects have damaged federal science agencies in their search for talent. DARPA has the authority to operate outside these restrictions, and the new technology entity will need similar powers if it is to ramp up quickly. Also important to the design of a new technology entity is the model DARPA has used for most of its history of independent project managers empowered with significant decisionmaking and budget authority. Where speed and innovation are priorities, a flat, empowered model trumps a tiered, bureaucratic model.

Nationwide outreach. DARPA's TRP demonstrated what a well-organized technology road show could accomplish for technology development. Cross-agency teams would travel and present threat problems and corresponding technology needs, aiming to encourage technologists and private-sector entrepreneurs to bring in new ideas and apply for funding awards or matches. For the technology entity, this "technology pull" exercise would help survey what approaches are available or could be rapidly developed, and help promote a face-to-face identification of available talent. We need aggressive outreach to solicit the best ideas from the best minds, not an armchair approach that waits for proposals to drift in.

Procurement flexibility. DARPA has the power to operate outside the traditional slow-moving federal procurement system and to undertake rapid and flexible R&D contracting. The homeland technology entity will need these same powers. It should have the ability to extend its procurement flexibility to sweep in cooperative

efforts with other entities, further encouraging other agencies to cooperate because they get access to new procurement powers.

Integrated development, deployment, evaluation, and testing. Whereas DARPA tries to integrate applied science with fundamental science to pursue breakthrough technologies, the homeland technology entity will have a more complex mission. In the long term, it will need to develop breakthrough technologies for homeland security, but in the short term it will need to survey and promote the deployment of existing technologies, often across agency lines. In addition, it will need to test and evaluate existing security capabilities as well as potential new systems. These tasks need to be integrated so that each stage can learn from the others. This complex array of technology tasks reinforces the argument that the new entity must have enough power to command respect and marshal cooperation from other parts of the government.

Governance. The new technology entity will need to pull other agencies into its governance structure to help enlist their cooperation through involvement and participation. It likely will work best if participating agencies feel shared ownership. This probably requires a bifurcated structure: (1) a council of senior S&T leaders from other mission agencies involved in homeland security for overall policy direction, and (2) working groups of project managers from affected agencies organized around developing detailed programs in each key threat area. A director with a strong technology development background could wield overall executive and administrative powers for the new entity, chairing the council and working with the entity's project managers, who would chair the working groups. The governance structure must create cooperative buy-in among agencies, which must see this as a shortcut to solving security problems they face in their jurisdictions. S&T can't be ordered into existence, they have to be nurtured.

Roadmap. An immediate task of this cooperative structure would be to develop a plan for finding and proposing deployment of

existing technology opportunities and developing new ones. Threats and vulnerabilities will have to be assessed and focus areas set. This could incorporate a classic technology road-mapping exercise. Provision will need to be made for updates and revisions as new threats and opportunities materialize. There can be no order in the current homeland technology chaos unless there is a coherent planning exercise. This planning will be a key mechanism for winning the allegiance of other agencies and fixing their technology roles and commitments.

The deployment dilemma. DARPA has long faced problems in persuading the armed services to deploy technologies it has developed, because DARPA can't control or significantly influence service acquisition budgets. A homeland technology entity faces similar problems in enticing a host of other agencies to adopt technologies it develops. Given the nation's vulnerabilities, we cannot afford to have a homeland technology entity face institutionalized technology transition barriers. Its parent homeland security agency must be able to influence the deployment budgets of involved mission agencies. In addition, the homeland agency may need a special technology transition fund to encourage deployment by these agencies. Regular reporting by the technology entity to the president and Congress on technology progress and opportunities could create additional awareness of research progress and corresponding pressure for prompt deployment.
The scope of the homeland security threat is so broad and deep that a new technology enterprise seems mandatory in facing it. Interestingly, the kind of model discussed here may have broader relevance. The U.S. science enterprise is still living under an organizational structure fixed in place a half century ago. Since then, scientific advance has increasingly required cross-disciplinary approaches, which in turn dictate cross-agency and public-private efforts. Yet we are not organized for these new kinds of approaches. A homeland technology entity, purposely created to cross agency, disciplinary, and sectoral lines and to

promote cooperation across these lines, could provide a model for a new kind of organization for the new S&T advances we must have in all areas.

Finally, we have discussed the security of the U.S. homeland throughout this piece, because our government is discussing the same conceptual framework. But we need to recognize that this is only part of the picture. A security system will not work if it stops at our borders. Like it or not, the United States is so inherently open and our vision so global in reach that our thinking about homeland security has to push out our concept of borders and contemplate global systems of security. Homeland must be very broadly defined.

This further complexity underscores the need for technology advances in obtaining higher security. The National Guardsmen now deployed at U.S. airports daily remind us that manpower alone will not ensure security. Technology deployment is crucial, and technology intensity will be as crucial to a new system of security for this new political landscape as it was for military superiority in the Cold War and the Gulf War. A new homeland technology entity based on a new organizational model will be central to that technology development and deployment. We need both new tools and new ways to build them.

Recommended reading

Department of Transportation Inspector General Web site, links to testimony, statements, and audits, including "Deployment and Use of Security Technology," before the House Committee on Transportation and Infrastructure, October 11, 2001, and "Status of Airline Security After September 11," before the Senate Committee on Governmental Affairs, November 14, 2001.

Stephen E. Flynn, "The Unguarded Homeland: A Study in Malign Neglect," in *How Did This Happen? Terrorism and the New War*, J. F. Hoge and G. Rose, eds. (Council on Foreign Relations, Inc., New York, 2001), 183–197.

House Committee on Transportation and Infrastructure Hearing, "Checked Baggage Screening Systems: Planning and Implementation for the December 31, 2002 Deadline," December 7, 2001.

T. O'Toole and T. Inglesby, *Shining Light on Dark Winter* (Johns Hopkins Center for Biodefense Studies, , 2001).
Potomac Institute for Policy Studies, *A Review of the Technology Reinvestment Project, PIPS-99-1, 1999*; and *A Historical Summary of the Technology Reinvestment Project's Technology Development, PIPS-96-1, 1996* (Arlington, Va.)

S.1764, Biological and Chemical Weapons Research Act, introduced by Sen. Joseph I. Lieberman; statement on bill introduction, *Congressional Record*, p. S12376-S12384, December 4, 2001.

Senate Committee on Governmental Affairs Hearings: "Has Airline Security Improved?" November 14, 2001; "Federal Efforts to Coordinate and Prepare the United States for Bioterrorism: Are They Adequate?" October 17, 2001; "Legislative Options to Strengthen Homeland Defense," October 12, 2001; "Critical Infrastructure Protection: Who's in Charge?" October 4, 2001; "Weak Links: How Should the Federal Government Manage Airline Passenger and Baggage Screening?" September 25, 2001; "Responding to Homeland Threats: Is Our Government Organized for the Challenge?" September 21, 2001; "How Secure is Our Critical Infrastructure?" September 12, 2001

William B. Bonvillian is legislative director and chief counsel to Sen. Joseph I. Lieberman of Connecticut. Kendra V. Sharp is an assistant professor of mechanical engineering at the Pennsylvania State University.