Deploying Homeland Security Technology

By: Albert N. Link and Vincent C. Henrich

Link, A.N, and V.C. Henrich (2003) Deploying homeland security technology. *J. Technol. Transfer* 28: 363-368. DOI: 10.1023/A:1024973701997

Made available courtesy of Springer Verlag: http://dx.doi.org/10.1023/A:1024973701997

Article:

Question: What do the Department of Homeland Security, Intel, and Disney have in common?[1] Answer: The success of each depends on how efficiently they implement new technologies. Although the White House and the Congress have responded swiftly to the events of September 11, 2001, the long-term security of our Nation, and thus the success of the newly created Department of Homeland Security, will depend in a substantial way on the efficiency with which technologies relevant to homeland security are created and, more importantly, deployed.

The purpose of this paper is to assess the Administration's revealed understanding of the innovation process, which underlies the creation of new homeland security technology, and attendant factors that relate to the efficiency with which the new technology is deployed. By "revealed understanding" we are referring to the written word, namely what is outlined in the Homeland Security Act of 2002 and related documents. Certainly, the Act, and related documents from the White House, are only initial templates that frame activities to come. But, as the Brookings Institution's (2002, p. i) early assessment of the Department's organization, and the Department's organization is fundamentally related to its ability to provide incentives for the creation and deployment of homeland security technology, " ... while it is possible to revisit or even reverse organizational decisions at a later stage, it is far better to get it right the first time."

An emphasis on homeland security technology

On June 6, 2002, President Bush addressed the Nation (Bush, 2002):

> So tonight, I ask the Congress to join me in creating a single, permanent department with an overriding and urgent mission: securing the homeland of America, and protecting the American people.
>
> The Department of Homeland Security will be charged with four primary tasks. The new agency will [1] control our borders and prevent terrorists and explosives from entering our country. It will [2] work with state and local authorities to respond quickly and effectively to emergencies. It will [3] bring together our best scientists to develop technologies that detect biological, chemical, and nuclear weapons, and to discover the drugs and treatments to best protect our citizens. And this new department will [4] review intelligence and law enforcement information from all agencies of government, and produce a single daily picture of threats against our homeland.

One of the first policy institutes to offer an opinion on homeland security was the Heritage Foundation (2002).[2] Its report, Defending the American Homeland, recommended four well conceived priorities: protecting the Nation's infrastructures, strengthening civil defense, improving intelligence and law enforcement, and military operations to combat terrorism.

The priorities introduced in the Heritage Foundation document were articulated in one form or another in the Administration's July 2002 National Strategy for Homeland Security. However, the two independent reports differ in one important respect. Defending the American Homeland ignored the role of technology in homeland security. Its implicit assumption was that new technologies would simply be available when needed to address appropriately the prioritized national needs. In contrast, National Strategy for Homeland Security explicitly addressed the important role of new technology.

National Strategy for Homeland Security sets forth a foundation for the Homeland Security Act of 2002, which was in draft form at the time of the report although the Act was not finalized until November. National Strategy for Homeland Security stated (p. 51):

> The Nation needs a systematic national effort to harness science and technology in support of homeland security. Our national research enterprise is vast and complex, with companies, universities, research institutes, and government laboratories of all sizes conducting research and development on a very broad range of issues.... The private sector has the expertise to develop and produce many of the technologies, devices, and systems needed for homeland security. The federal government needs to find better ways to harness the energy, ingenuity, and investments of private entities for these purposes.

The Homeland Security Act of 2002, Public Law 107–296, was passed on November 25, 2002. Section 101 (b) (1) states the mission of the newly created Department is to:

(A) prevent terrorist attacks within the United States;
(B) reduce the vulnerability of the United States to terrorism;
(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;
(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;
(E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;
(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland; and
(G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

The Act elaborates on the technology issues in National Strategy for Homeland Security in several respects, emphasizing in particular the terms "research" and "development." Section 302 gives the Directorate for Science and Technology within the Department responsibility for, among other things:[3]

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any of all elements of the Department, through both intramural and extramural programs ... ;
(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—
  (A) preventing the importation of chemical, biological, radiological, nuclear, and related weapons and materials; and
  (B) detecting, preventing, protecting against, and responding to terrorist attacks;
(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;

The Directorate for Science and Technology is also given the responsibilities for the operation of the newly established Homeland Security Advanced Research Projects Agency—HSARPA (Section 307 (b) (3)) to:[4]

(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;
(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies; and
(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.

An emphasis on university-based research, which was explicit in National Strategy for Homeland Security, is also noted in Section 308 (b) (1) of the Act with reference to the above referenced extramural programs. The Secretary, acting through the Under Secretary for Science and Technology:

... shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—
(A) ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practical participate;
(B) ensure that the research funded is of high quality
. . . ;
(C) distribute funds through grants, cooperative agreements, and contracts.

Is addition, university-based centers for homeland security will be established to coordinate university-based technology activities (Section 308 (b) (2)).

Section 312 (c) establishes the Homeland Security Institute, an organizational initiative that was not explicit in National Strategy for Homeland Security. The Institute will be responsible for, among other things:

(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders. 5,6

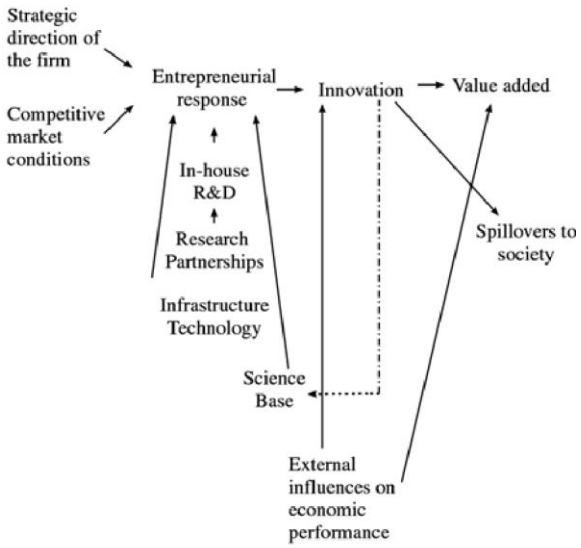
Innovation, technology, and the entrepreneurial process

To assess the Administration's emphasis on technology, a model of what we call the entrepreneurial process is offered and then the elements of that model are compared to the elements of technology creation and deployment set forth in the Act. The model is illustrated in Figure 1.

Briefly, the firm is characterized in the figure as an entrepreneurial agent of change, or, to reflect on terminology from this history of economic thought on entrepreneurship, the firm is characterized as the economic agent adjusting to disequilibria (Hebert and Link, 1988). The firm, as illustrated by the upper horizontal elements in the figure, optimizes given its strategic focus and the competitive pressures it faces in the marketplace, an,d of course, these two forces are interrelated although they are shown separately in the figure. Optimization generates an entrepreneurial response, and that purposive action in turn results in an innovation. There are additional market forces at work that are, in part, beyond the influence of the firm. These forces determine the economic value of the innovation and hence, the value added by the firm as well as to the user of the innovation.

Research and development (R&D) activity is the primary resource that the firm relies upon to investigate the appropriate strategic/market response and to act upon it. Enhancing the firm's R&D activity is the firm's relationship with other organizations as well as with its external environment. One such relationship is its involvement with other firms, or perhaps with either a university or a federal laboratory. Such strategic

associations are frequently referred to as research partnerships. Also, firms rely on infrastructure technologies (e.g. standards and protocols) that come from federal laboratories, or perhaps even from the environment created by being located in a science park. The science base, which consists of the stock of knowledge generated from basic research, resides in the public domain—and the public domain is international in scope—generally in the form of scientific journals but also it is in part embodied in university scientists.



Source: Feldman *et al.* (2002) and Link and Siegel (2003).

Figure 1. The entrepreneurial process.

As illustrated, the result of the entrepreneurial process is innovation. An innovation will generate value added if it is accepted in the marketplace. Furthermore, it will diffuse into society and generate spillover benefits to other firms both within the industry and in outside industries that ultimately use the innovation. The dashed arrow coming back to the science base shows an internal feedback. Once an innovation exists, knowledge has been created and it too will reside in the public domain.

All of the elements in the model in Figure 1 are touched upon in the Act. There is an explicit recognition in the Act that new homeland security technologies will be needed; that will come from myriad sources including firms but also universities and research institutions; and that the effective deployment of these technologies will depend on the availability of standards and protocols to help to ensure interoperability. Thus, high marks are given to the Administration for its implicit understanding of the critical elements that enhance the innovation process.[7,8]

However, two issues remain, and neither issue is addressed in the Act or in subsequent Administration white papers.[9] Specifically: What is the most effective way to organize the Department to maximize (1) the efficiency with which new technology is created and (2) the speed with which new technology is deployed and then effectively used for homeland security. The creation of new technology is common to all R&D agencies. The somewhat unique aspect of the Department of Homeland Security is the emphasis on deployment for immediate and future use, with a research strategy to evolve more slowly. One implication of this latter emphasis is the need to push technical infrastructure, and ultimately standards, to support deployment.

Some within the Technology Administration of the Department of Commerce have argued that, from a technology creation perspective, the Department of Homeland Security should model itself after the Defense Advanced Research Projects Agency (DARPA).[10] We disagree, as discussed in the following

section. To this point, no initiatives that have been suggested for how to increase the speed with which new technology is deployed and then effectively used.

The DARPA model[11]

On February 7, 1958, by Public Law 85-325 and Department of Defense Directive 5105.15, the Advanced Research Projects Agency (ARPA) was created and charged with the responsibility "for the direction or performance of such advanced projects in the field of research and development as the Secretary of Defense shall, from time to time, designate by individual project or by category." More specifically, the agency was created as a U.S. response to the Soviet launch of Sputnik. Among ARPA's founding principles, its activities will be project based, with a 3- to 5-year time horizon, and with a strong focus on end goals.

On March 23, 1972, ARPA's name was changed to DARPA, moving the agency under the Office of the Secretary of Defense. At that time its emphasis was on energy, information processing, and tactical technologies. But then on February 22, 1993, the name was changed back to ARPA during the Clinton administration. On February 10, 1996, the name was again re-changed to DARPA under Public Law 104–106. Throughout the 1990s ARPA/DARPA focused in the areas of materials science, electronic sciences and systems, information technology, and sensor technology.

While DARPA has been successful in generating and deployment technologies that it deemed important, the DARPA model is one that is solicitation based. This means that needed technologies are defined, such technologies are specified and solicited, and then DARPA becomes the market for new technologies. We are not critical of this model, in concept, because it seems to have worked well for DARPA for more than four decades.[12]

A solicitation-based program assumes that the solicitor can (1) define the needed technical requirements, (2) specify the physical representation of those requirements, and (3) determine when the technology will be needed to meet a particular need. Unfortunately, none of these three assumptions apply to homeland security technology.

Recommendations for the homeland security institute

While no initiatives have been put forward to increase the speed with which new technology is deployed and then effectively used, the Act does set forth an appropriate institutional umbrella to address this issue. The Homeland Security Institute is charged with identifying instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for filed operators and first responders. We recommend that the Institute do more than identify needed standards for "tools developed;" we recommend that it take on the role of an information broker. Specifically, the Institute could establish effective communications channels through which scientists and engineers could articulate infrastructure needs—standards—that they expect would be needed to bring to market technologies that they think may be relevant to homeland security, and scientists in our federal laboratory system could publicize the resource base of their expertise in various standards development areas. Such a communications role would have several distinct economic advantages.[13] But, information has to be provided to help these "actors" identify where and how to apply their comparative advantages. The implication is a need for strategic planning, including an assessment of the "security industrial base" (just as the Department of Defense assesses the "defense industrial base"). After all, deployment has to have end points and many of these end points are not pure private markets.

Our recommendation would allow all the relevant players on the homeland security field— scientists and engineers in universities, industry, and federal laboratories—to work in the area of their comparative advantage. It would serve an important public sector objective: to make accessible science-based information (as opposed to creating it). It would enhance market mechanisms rather than altering or replacing them. And finally, it would reduce the risk of government's intervening too much or too little.[14]

Acknowledgments

Earlier versions of this paper have benefited from the comments and suggestions of Connie Jacobs, Jamie Link, John Roberts, Greg Tassey, Eleanor Thomas, and Don Siegel.

Notes:

1. This introduction format is borrowed from "Bully for Brontosaurus" (Gould, 1991).
2. The Heritage Foundation Homeland Security Task Force was independently formed shortly after the events of September 11.
3. The directorate will be headed by an Under Secretary for Science and Technology.
4. The 2003 budget for this agency is authorized at $500 million "and such sums as may be necessary thereafter" (Section 307 (c) (2)).
5. Standards have long been known to be critical to the speed at which new technologies enter the marketplace (Link and Tassey, 1988; Link and Kapur, 1994) and then to their effective use. Regarding the latter, "In 1904, a fire broke out in the basement of the John E. Hurst & Company Building in Baltimore [Marylandl. After taking hold of the entire structure, it leaped from building to building until it engulfed an 80-block area of the city. To help combat the flames, reinforcements from New York, Philadelphia and Washington, DC immediately responded—but to no avail. Their fire hoses could not connect to the fire hydrants in Baltimore because they did not fit the hydrants in Baltimore. Forced to watch helplessly as the flames spread, the fire destroyed approximately 2,500 buildings and burned for more than 30 hours." See: http://www.ansi.org/ consumer_affairs/history_standards.aspx?menuid = 5 This Baltimore event was instrumental in the formation of the National Bureau of Standards, which later became the National Institute of Standards and Technology (NIST).
6. The importance of the proposed Institute was emphasized by the National Research Council (2002).
7. The Brookings Institution offered an organizational criticism of the organization of the Department of Homeland Security, noting that the Department's narrow focus on chemical, radiological, biological, and nuclear countermeasures research ignores the wide contribution that science and technology could make to secure the Nation against terrorism.
8. Section 1003 of the Act makes clear the potential role of the NIST in developing standards for information systems, but NIST's standards and protocol general expertise could be equally as relevant to many other technologies.
9. Surprisingly, neither of these issues was addressed by the Brookings Institution in their critique of the organization of the Department of Homeland Security (2002) or in RAND's December 2002 report to the President.
10. Personal correspondence.
11. Much of the material in this section comes directly from the DARPA Web site: http://www.darpa.mil
12. In contrast, the Potomac Institute for Policy Studies (2001) points out that DARPA's history of pursuing radical innovations and technologies results in them being "difficult to deliver and to transition" (p. x).
13. This recommendation assumes, of course, that the research sector is not only capable of producing needed technologies but also that it is capable of anticipating what technologies will be needed in the future.
14. There are within the Act resources on call to accomplish my recommendation. Section 308 (c) gives the Department authority to create intramural research programs using the resources of, say, the federal laboratory system. National Strategy for Homeland Security (2002) calls for the establishment of a national laboratory for homeland security and my recommendation could become part of that infrastructure's mission.

References

Brookings Institution, 2002, *Assessing the Department of Homeland Security*, Washington, DC: The Brookings Institution.

Bush, President George W., 2002, 'Remarks by the President in Address to the Nation,' http://www.whitehouse.gov/news/release/2002/06/20020606-8.html.

Feldman, M., A.N. Link, and D.S. Siegel, 2002, *The Economics of Science and Technology*, Norwell, MA.: Kluwer Academic Publishers.

Gould, S.J., 1991, *Bully for Brontosaurus: Reflections in Natural History*, London: W.W. Norton.

Hebert, R.F. and A.N. Link, 1988, *The Entrepreneur: Mainstream Views and Radical Critiques*, New York: Praeger Publishers.
Heritage Foundation, 2002, *Defending the American Homeland*, Washington, DC: The Heritage Foundation.
Link, A.N. and P. Kapur, 1994, 'A Note on the Diffusion of FMS Technology,' *Economics Letters* 369–374.
Link, A.N. and D.S. Siegel, 2003, *Technological Change and Economic Performance*, London: Routledge.
Link, A.N. and G. Tassey, 1988, 'Standards and the Diffusion of Advanced Technologies,' *Evaluation and Program Planning*, 97–102.
National Research Council, 2002, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, DC: National Academies Press.
Office of Homeland Security, 2002, *National Strategy for Homeland Security*, Washington, DC: Office of Homeland Security.
Potomac Institute for Policy Studies, 2001, *Transitioning DARPA Technology*, Arlington, VA: Potomac Institute for Policy Studies.
RAND, 2002, Implementing the National Strategy, Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Arlington, VA: RAND.