Backgrounder

Published by The Heritage Foundation

No. 1977
October 5, 2006
Updated October 19, 2006

Homeland Security Technology, Global Partnerships, and Winning the Long War

James Jay Carafano, Ph.D., Jonah J. Czerwinski, and Richard Weitz, Ph.D.

Countries have limited financial, human, and other resources available for homeland security. Winning the long war to disrupt transnational terrorist networks will require international collaboration in researching, developing, and sharing homeland security technologies. By facilitating greater cooperation, spreading research and development (R&D) costs, and taking advantage of synergies, the United States and its allies can extend the impact of their homeland security programs, entice businesses and entrepreneurs with larger numbers of potential customers, and take advantage of the continuing internationalization of the global market for security technologies.

Whither Washington?

The U.S. government spends considerably more money on developing homeland security technologies than is spent by any other national government. The Department of Homeland Security Appropriations Act of 2006[1] allocated approximately $6 billion for homeland security technologies, primarily for applying technologies rather than conducting basic research. Major projects include introducing detectors for finding smuggled nuclear matter, consolidating data networks, defending against biological terrorism, and upgrading border security controls under the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program.[2]

Homeland security R&D spending totals about $4 billion annually, and the Department of Homeland Security (DHS) manages approximately one-third of

Talking Points

- America's homeland security technology is currently developed by a number of U.S. agencies, but a country's resources by themselves will not be enough to combat terrorism. To meet the threat, technology sharing should be a priority.
- The U.S. shares some technology with friends and allies but has yet to develop a system that promotes sharing of research across the borders.
- The DHS's most urgent task is to develop an international science and technology strategy to improve the coherence of the department's foreign efforts, including the sharing of critical homeland security technologies.
- DHS reforms should also encourage the development of more technologies and the exchange of new ideas. In particular, the DHS needs to establish a clearinghouse of existing technologies that describes the technologies, their capabilities, and their possible missions.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1977.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

that amount.[3] The Homeland Security Act of 2002[4] charged the DHS with coordinating federal efforts to produce and deploy the best available technologies for homeland security missions. The Science and Technology (S&T) Directorate's R&D budget for fiscal year 2006 was almost $1.4 billion. Half of this total goes to developing countermeasures against chemical, biological, radiological, nuclear, and high-explosive weapons. Other large S&T programs are for developing technologies to defend commercial aircraft from surface-to-air missiles, to track nuclear objects (the core mission of the newly established Domestic Nuclear Detection Office), and to secure cargo containers.

The S&T Directorate researches, develops, and tests homeland security technologies. The DHS awards grants to universities researching new homeland security technologies; has established Centers of Excellence at several American universities;[5] and funds technical and organizational initiatives among federal, state, and local emergency responders, such as the Regional Technology Integration initiative.[6] The DHS also works with private-sector industry and academic institutions to adapt technologies for use by federal, state, and local officials and emergency responders.[7]

Other federal departments and agencies also serve key roles in researching and developing homeland security technologies, especially the Department of Defense (DOD), the Department of Health and Human Services (HHS), and the national laboratories run by the Department of Energy. For example, the Advanced Portal Security system developed by the Defense Advanced Research Projects Agency endeavors to identify concealed containers of chemical and biological agents by rapidly detecting chemical and biological agents on people and inside envelopes, small containers, and packages. The HHS's Bioshield works to provide incentives for the private sector to develop and manufacture vaccines against biological agents, and the Los Alamos National Laboratory and Lawrence Livermore National Laboratory jointly run the Biological Aerosol Sentry and Information System (BASIS) to develop ways to detect airborne biological weapons attacks.

Several efforts are underway to coordinate interagency efforts to research and develop homeland security technologies. The Homeland Security Council establishes general guidelines for all U.S. homeland security policies.[8] The director of the White House Office of Science and Technology Policy advises the President on homeland security issues. The Technical Support Working Group (TSWG), operated jointly by the State Department and DOD, oversees interagency R&D programs

1. Public Law 109–90.
2. Wilson P. Dizard III, "DHS Spending Bill, Now Law, Bolsters Technology," *Government Computer News*, October 19, 2005, at *www.gcn.com/online/vol1_no1/37331-1.html?topic=homeland-security* (August 8, 2006).
3. Genevieve J. Knezo, "Homeland Security Research and Development Funding, Organization, and Oversight," Congressional Research Service *Report for Congress*, June 9, 2005.
4. Public Law 107–296.
5. Major universities heading Center of Excellence partnerships include John Hopkins University, University of Southern California, Texas A&M University, University of Maryland, and Michigan State University. For more information, see U.S. Department of Homeland Security, "Research & Technology," at *www.dhs.gov/dhspublic/interapp/editorial/editorial_0498.xml* (August 8, 2006).
6. The Regional Technology Integration Initiative (RTII) is set up to "facilitate the transition of innovative technologies and organizational concepts to regional, state, and local jurisdictions." RTII will enable state and local agencies to feed "boots on the ground" input into the science and technology community at DHS for areas such as disaster response, providing a communication channel in order for technologies to better fit requirements at the ground level. For more information, see U.S. Department of Homeland Security, "Fact Sheet: Regional Technology Integration Initiative," June 7, 2004, at *www.dhs.gov/dhspublic/display?content=3704* (August 8, 2006).
7. Daniel Morgan, "Research and Development in the Department of Homeland Security," Congressional Research Service *Report for Congress*, updated June 20, 2003, at *www.fas.org/man/crs/RL31914.pdf* (September 26, 2006).

designed to develop and deploy counterterrorism technologies. Its executive committee has representatives from the Departments of State, Defense, Justice, and Energy. The DHS also participates in TSWG contract solicitations. Although the TSWG works with a broad range of private-sector actors, they reside predominately in the United States and a few select partner countries. In addition, TSWG efforts focus primarily on meeting members' immediate operational needs by adapting commercial off-the-shelf technology.

More recently, the White House established a new national organization to lead the development and acquisition of technology focused on detecting smuggled nuclear material. Created in April 2005 pursuant to Homeland Security Presidential Directive 14,[9] the Domestic Nuclear Detection Office (DNDO) commands a budget of approximately $500 million and a staff of nearly 200 from the Departments of Homeland Security, Defense, and Energy and the FBI. In July, Homeland Security Secretary Michael Chertoff and DNDO Director Vayl Oxford announced over $1 billion in new investments to strengthen nuclear detection. A Cabinet-level Interagency Coordination Council informs the R&D investments of the new office to reinforce government-wide returns. Additionally, the DNDO is responsible for designing an interagency-approved "global architecture" to guide the strategies for deploying nuclear detection capabilities overseas as well as domestically.[10]

Allied Action

Other countries spend much less than the United States spends on homeland security S&T programs.[11] Although the European Union launched a Security Research Program in March 2003 to fund homeland security R&D, the program focuses on enhancing protection of critical transportation infrastructure (e.g., railroads, ports, airlines, and information networks) and not on developing new capabilities for emergency responders.[12] In addition, European homeland security projects remain highly fragmented, with different EU bodies and member country agencies having disparate authorities and competencies. These problems raise the specter of a growing capabilities gap in homeland security technologies that would compound U.S.–European disparities in other defense areas.[13]

8. For one such set of requirements, see George W. Bush, "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive HSPD-12, at *www.whitehouse.gov/news/releases/2004/08/20040827-8.html* (August 8, 2006). All 14 Homeland Security Presidential Directives contain such requirements standards to some extent.
9. George W. Bush, "Domestic Nuclear Detection," National Security Presidential Directive NSPD-43/Homeland Security Presidential Directive HSPD-14, April 15, 2005, at *www.fas.org/irp/offdocs/nspd/nspd-43.html* (September 28, 2006). See U.S. Department of Homeland Security, "Fact Sheet: Domestic Nuclear Detection Office," April 20, 2005, at www.*dhs.gov/dhspublic/display?content=4474* (August 8, 2006).
10. For more information, see Michael L. Moodie, "A Long-Term Response to Biological Terrorism: Homeland Security Leaders Need Shared Intellectual Framework and Greater International Cooperation," Center for the Study of the Presidency *Issue Paper* No. 12, August 2005, at *www.thepresidency.org/pubs/IssuePaper12.pdf* (August 8, 2006).
11. For instance, for spending data on British efforts, see U.K. Home Office, "Security," at *www.homeoffice.gov.uk/security/protecting-the-uk/?version=1* (August 8, 2006). For a review of German efforts, see Thania Paffenholz, Ph.D., and Dunja Brede, "Lessons Learnt from the German Anti-Terrorism-Package (ATP)," Deutsche Gesellschaft für Technische Zusammenarbeit, 2004, at *www.gtz.de/de/dokumente/en-atp.pdf* (August 8, 2006), and Francis Miko and Christian Froehlich, "Germany's Role in Fighting Terrorism: Implications for U.S. Policy," Congressional Research Service *Report for Congress*, December 27, 2004, at *www.fas.org/irp/crs/RL32710.pdf* (September 28, 2006).
12. Gerd Foehrenbach, "Transatlantic Homeland Security and the Challenge of Diverging Risk Perceptions," in Esther Brimmer, ed., *Transforming Homeland Security: U.S. and European Approaches* (Washington, D.C.: Center for Transatlantic Relations, 2006), p. 52. For information on EU programs, see European Commission, "Security Research," at *http://ec.europa.eu/enterprise/security/index_en.htm* (August 8, 2006), and press release, "13 New Security Research Projects to Combat Terrorism," European Commission, August 2, 2005, at *http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/277* (August 8, 2006).

Individual countries have also made contributions to advancing homeland security technologies. For example, some European governments maintain centralized clearinghouses of technologies and best practices designed to enhance rail security in addition to conducting centralized research and testing of promising defense technologies.[14] European countries are also on the cutting edge of investigating the application of biometric technologies.[15]

Several European governments have made a special effort to cultivate niche capabilities in areas relevant to homeland security. For example, during Operation Enduring Freedom, the Czech Republic, Germany, and Italy agreed to send their specialized chemical and biological detection units to supplement U.S. defenses.[16] More recently, the Czech government created a Chemical, Biological, Radiological, and Nuclear (CBRN) Center of Excellence. In April, the U.K. Ministry of Defence stood up its Counter-Terrorism Science and Technology Centre. The Underwater Research Center in Italy is leading a series of technology tests to develop enhanced port, harbor, and vessel security through capabilities such as underwater autonomous vehicles and sensor networks.

Nevertheless, European governments generally devote modest resources to capabilities and technologies relevant to homeland security. Although the demand for homeland security technology in Europe is expected to grow to over 874 million euros (almost $1.2 billion) in the next 10 years,[17] the U.S. government still invests 50 percent more in science and technology R&D than Europe invests.[18]

In contrast, global private-sector spending for homeland security R&D has experienced exponential growth—a trajectory that analysts expect to continue. According to one projection, international commerce in antiterrorist equipment and consulting services will soar from $46 billion in 2005 to $178 billion by 2015, with the United States accounting for half the market.[19] This figure is even larger if spending on technologies developed primarily for military or law enforcement purposes (some of which can contribute to homeland security) and private-sector spending for critical infrastructure protection are included.

Cooperation Across Borders

The United States maintains strong bilateral R&D relationships with several countries. Israeli–American security cooperation is an important example of a successful relationship. The Israelis' decades-long struggle against terrorist attacks has led them to develop innovative countermeasures. For instance, they first used x-ray machines to in-

13. For a review of U.S.–European disparities in traditional military technologies, see David S. Yost, "The NATO Capabilities Gap and the European Union," *Survival*, Vol. 42, No. 4 (December 2000), pp. 97–128. For ways to reduce the gap, see Donald C. Daniel, "NATO Technology: From Gap to Divergence?" *Defense Horizons*, No. 42 (July 2004), at *www.ndu.edu/ctnsp/defense_horizons/DH42.pdf* (August 8, 2006).
14. U.S. Government Accountability Office, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO–06–181T, October 2005, at *www.gao.gov/new.items/d06181t.pdf* (September 28, 2006). Although the researchers acknowledge that political, legal, fiscal, and cultural differences between countries would complicate efforts to apply foreign practices for domestic use without modification, such differences also ensure the availability of a diverse range of homeland security experiences, some of which might be suitable for foreign application.
15. European Biometrics Portal, *Biometrics in Europe: Trend Report*, European Community, June 2006, at *www.europeanbiometrics.info/images/resources/112_165_file.pdf* (September 28, 2006).
16. Tomas Valasek, "The Fight Against Terrorism: Where's NATO?" *World Policy Journal*, Vol. 18, No. 4 (Winter 2001/02), p. 21, at *www.worldpolicy.org/journal/articles/wpj01-4/Valasek.pdf* (September 28, 2006).
17. Frost & Sullivan, "European Homeland Security Boosting Demand for Security Technologies, Says Frost," Tekrati, January 10, 2006, at *www.tekrati.com/research/News.asp?id=6285* (August 22, 2006).
18. John H. Marburger III, Director, Office of Science and Technology Policy, "Fiscal Year 2006 Appropriations," testimony before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, March 11, 2005.
19. Susan Karlin, "Get Smart," *Forbes*, December 12, 2005, p. 81.

spect airplane luggage and pioneered placing air marshals on every commercial flight of their national airline. More recent Israeli inventions include guns that shoot around corners, laser units that can detect explosives from distances of hundreds of feet, and computer software capable of translating dog barks into English-language commands.[20]

In 1995, the U.S. and Israel established the United States–Israel Science and Technology Foundation (USISTF), a bilateral initiative to increase technology sharing. In June 2005, USISTF sponsored a conference in Jerusalem that brought together top executives of large U.S. corporations, influential American government officials, and other key U.S. homeland security players with leaders of the Israeli defense and security industries.[21] Israel has also shared counterterrorist technologies with India, Turkey, and other countries.

Most U.S. efforts in this area remain ad hoc and focused on a few traditional key partners such as Britain and Canada. For example, a 2004 memorandum of agreement signed by then-DHS Deputy Secretary James Loy and British Home Secretary David Blunkett created a cooperative S&T framework in critical infrastructure protection and other homeland security sectors. The memorandum established formal exchanges of scientists, engineers, and other specialists working in this area. It also set criteria for harmonizing standards and guidelines for homeland security technologies.[22]

Canadian–U.S. cooperation in homeland security technology R&D is perhaps even more extensive. In June 2003, the DHS and Defence R&D Canada launched a Public Security Technical Program to pursue S&T solutions across many homeland security dimensions. On June 1, 2004, the two governments signed the Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security, which provides a framework for joint security S&T projects in these two areas.[23]

Outside of strong bilateral research programs with countries like Great Britain and Israel, formal initiatives are much less robust and are largely holdovers from the Cold War and a long-standing relationship with NATO. Even with NATO, cooperation has always been modest. NATO traditionally considers developing, equipping, training, maintaining, and financing military capabilities to be primarily national responsibilities.

In terms of developing NATO capabilities for homeland security and consequence management, the Conference of National Armament Directors (CNAD) and its subordinate bodies play an important role. The CNAD consists of national armaments directors who meet regularly to identify opportunities for allied collaboration in researching, developing, and producing military equipment.

The NATO Industrial Advisory Group (NIAG) enables the CNAD to solicit industry advice on how to promote public–private and transnational cooperation in defense production. For example, the NIAG is currently coordinating private industrial involvement in NATO's Defense Against Ter-

20. *Ibid.*

21. For a description of the conference, see United States–Israel Science and Technology Foundation, "The Jerusalem Conference on Homeland Security," at *www.usistf.org/Jerusalem_Conference.htm* (August 8, 2006).

22. Joe Pappalardo, "Britain and U.S. Agree to Share Security Tech," *National Defense*, Vol. 89, No. 615 (February 2005), p. 10. Nevertheless, British–American cooperation on traditional military technologies remains far more extensive than cooperation in the homeland security realm, and major problems persist even in this area. See Pierre Chao and Robin Niblett, "Trusted Partners: Sharing Technology Within the U.S.–U.K. Security Relationship," Center for Strategic and International Studies *Working Paper*, May 26, 2006, at *www.csis.org/media/csis/pubs/060526_usukpartnersreport.pdf* (September 28, 2006).

23. For the text of the agreement, see Agreement Between the Government of the United States of America and the Government of Canada for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security, December 12, 2001, at *www.pstp.drdc-rddc.gc.ca/bordersecurity_60104.pdf* (August 8, 2006). For additional background information, see Canadian Secretariat of the Public Security Technical Program, "Public Security Technical Program," Web site, at *www.pstp.drdc-rddc.gc.ca/home_e.asp* (August 8, 2006).

rorism program. Such cooperation has already yielded new technologies to defend against improvised explosive devices.[24]

The NATO Research and Technology Organization annually sponsors over 100 cooperative activities among alliance members and partners, primarily in the area of basic research.[25] Allied Command Transformation has the lead responsibility for implementing defense innovation within NATO, including encouraging experimentation and advanced technology demonstrations.[26]

NATO's WMD Centre, created in 2000, supports NATO initiatives to address the threat of weapons of mass destruction (WMD) across the 46 countries involved in the Euro–Atlantic Partnership Council (EAPC), including the seven Middle Eastern countries participating in NATO's Mediterranean Dialogue.[27] Moreover, NATO this year appointed a Counterterrorism Technology Coordinator after standing up the new NATO Counterterrorism Technology Unit.

After 9/11, the NATO heads of state and government adopted a Civil Emergency Planning (CEP) Action Plan at their November 2002 Prague Summit, listing over 50 action items designed to assist EAPC governments' civil preparedness against CBRN agents. In their summit declaration, NATO members expressed their commitment to "enhance our ability to provide support, when requested, to help national authorities to deal with the consequences of terrorist attacks, including attacks with CBRN against critical infrastructure, as foreseen in the CEP Action Plan." The plan's objectives include improving interoperability among NATO member and partner countries by setting common minimum standards for equipment, planning, training, and procedures.

The Prague Summit participants also approved a Partnership Action Plan against Terrorism (PAP-T),[28] which contains several provisions designed to enhance technology cooperation in homeland security among EAPC members. Summit participants also agreed on a program of Nuclear, Biological, and Chemical Defense Initiatives to improve defenses for NATO troops and citizens against such attacks. For example, they launched a NATO-wide Disease Surveillance Initiative to monitor unusual disease outbreaks, alert alliance leaders about biological outbreaks, and fuse data with other information sources. They also established a coordinated stockpile of materials for chemical and biological defense. This NATO Biological–Chemical Defense Stockpile allows member governments to pool their resources (e.g., vaccines and protection gear) by identifying and sharing national supply inventories, rapidly moving needed materials, and sharing information on improving medical treatment protocols.

In May 2004, NATO launched a Programme of Work for Defense Against Terrorism to strengthen the protection of allied populations and troops from terrorist attacks. The program consists of priority armaments projects, each led by a member country, designed for specific terrorist threats. NATO has also reoriented its sci-

24. Nicholas Fiorenza, "European Research Is Yielding a Bevy of Anti-IED Technologies," *Aviation Week & Space Technology*, May 22, 2006, p. 534.

25. For a survey of the RTO and its activities, see North Atlantic Treaty Organization, "RTO—The Research and Technology Organisation," at *http://ftp.rta.nato.int/public/Documents/RTO/RTO-Pamphlet.pdf* (August 8, 2006).

26. North Atlantic Treaty Organization, Supreme Allied Commander Transformation Headquarters, "Allied Command Transformation: Fact Sheet," November 2005, at *www.act.nato.int/multimedia/facts/FACT%20SHEET%20-%20ACT%20Nov%202005.pdf* (August 22, 2006).

27. NATO has yet to fully extend counter-WMD and anti-WMD efforts in those countries participating in the Istanbul Cooperative Initiative.

28. For the text of the PAP-T, see North Atlantic Treaty Organization, "Partnership Action Plan against Terrorism," updated January 22, 2003, at *www.nato.int/docu/basictxt/b021122e.htm* (August 8, 2006). For a discussion of the document and the projects it subsequently generated, see Osman Yavuzalp, "Working with Partners to Fight Terrorism," *NATO Review*, Issue 1 (Spring 2003), at *www.nato.int/docu/review/2003/issue1/english/art3_pr.html* (August 8, 2006).

ence initiatives into the Security Through Science program to focus investments on improved counterterrorism and antiterrorism capabilities across NATO.

Outside of NATO, U.S. cooperation with friends and allies in homeland security S&T is much less robust. At present, such collaboration occurs largely at industry-sponsored events, such as the annual International Asia Homeland Security Exhibition and Conference, attended by law enforcement representatives and counterterrorism experts.[29] However, certain formal cooperative institutions do exist, such as the trilateral U.S.–Canada–Mexico Security and Prosperity Partnership of North America, which use trade regulations to enhance their ability to share technology and mitigate the risk of terrorism to North America.

Shortfalls and Shortcomings

The DOD's June 2005 strategy document for homeland defense states:

> The Department of Defense seeks to improve the homeland defense and homeland security contributions of our domestic and international partners and, in turn, to improve DOD capabilities by sharing expertise and technology, as appropriate, across military and civilian boundaries.[30]

Although the United States and its allies participate in a number of ongoing domestic and international programs, they have yet to develop a strategic vision or comprehensive mechanism to promote the sharing of international technology for homeland security. Unlike processes for sharing defense technologies, which emerged over decades of cooperation among allies during the Cold War, the sharing of homeland security technology remains in its infancy. A 2004 General Accounting Office report found that the DHS had made little progress in crafting a comprehensive long-range plan for developing CBRN countermeasures. It also concluded that DHS R&D coordination with other federal agencies remains suboptimal.[31] Unlike the DOD, the DHS has not developed an explicit international science and technology strategy.[32] Congress has also expressed frustration over how slowly the DHS has certified and deployed new technologies.[33]

While bilateral arrangements serve a purpose, the DHS needs to widen and deepen its level of technical cooperation with foreign countries. Thus far, it has focused overwhelmingly on promoting the transfer of homeland security technologies among domestic U.S. entities. The DHS has established an international affairs office, but the office has failed to reduce the fragmented nature of the department's foreign-oriented activities.

The lack of a technology clearinghouse that highlights specific technologies and explains what the technology is and what missions it can perform hinders progress in clearly defining and creating a strong security technology development regime. Establishing a technology clearinghouse would enable partners to know what technologies are available for transfer; provide a method of setting standards so that technologies are understandable; create an interoperable and

29. For more on the International Asia Homeland Security Exhibition and Conference, also known as the Safety and Security Asia Conference, see "Safety & Security Asia 2007," Web site, at *www.safetysecurityasia.com.sg* (August 8, 2006).

30. U.S. Department of Defense, "Strategy for Homeland Defense and Civil Support," June 2005, p. 2, at *www.fas.org/irp/agency/dod/homeland.pdf* (September 28, 2006).

31. Specifically, the report urged the DHS to coordinate and utilize laboratories in the Department of Energy. See U.S. General Accounting Office, *DHS Needs a Strategy to Use DOE's Laboratories for Research on Nuclear, Biological, and Chemical Detection and Response Technologies*, May 2004, p. 22, at *www.gao.gov/new.items/d04653.pdf* (August 22, 2006). The General Accounting Office was renamed the Government Accountability Office in July 2004.

32. See U.S. Department of Defense, Defense Research and Engineering, "International Science and Technology Strategy for the United States Department of Defense," April 2005.

33. For example, see Harold Rogers, "Remarks of Chairman Harold Rogers FY 2006 Homeland Security Subcommittee Mark Up," States News Service, May 4, 2005.

transferable means for industry-to-industry dialogue; establish predictable export control requirements; and construct acquisition mechanisms such as joint development programs, licensing agreements, and something comparable to the foreign military sales program.[34]

Another challenge is that programs in NATO, potentially the United States' most important partner, have developed slowly. NATO programs lack funding and dedicated test facilities and training ranges.[35] In addition, significant problems (such as concerns about protecting privacy and intellectual property) continue to impede transatlantic security cooperation against terrorists and other unconventional threats.[36]

Finally, NATO does a poor job of leveraging research and development in the private sector. Assistant Secretary General of NATO Marshall Billingslea has pointed out:

> Across North America and Europe, there are tens of thousands of large and small companies, universities, government institutes and—in some cases—garages and hobby shops of inventors, all of whom have something to offer the fight against terrorism. The inventiveness and creativity of our private sectors is one of the greatest assets NATO nations have in the fight against terrorism. We need to do a better job of tapping into that creativity.[37]

To date, however, NATO as an organization has developed mechanisms to engage the private sector, but member states have done little to make use of that potential.

Options and Ideas

The DHS's most urgent task is to develop an international science and technology strategy to improve the coherence of the department's foreign efforts, including the sharing of critical homeland security technologies.[38]

Domestically, the DHS and DOD should build cooperative partnerships. A report by the Board on Army Science and Technology explained how the Army could support homeland security and made recommendations for the Army that would "ensure a high level of interoperability between emergency responders and the Army."

Expanding these recommendations across the DOD spectrum would create a laudable framework for DHS–DOD technology collaboration and sharing. They include working together to "determine appropriate planning processes necessary to determine which…science and technology programs should be shared and how best to go about doing this."[39] Programs covered in the report range from communications for emergency responders to nuclear, radiological, and explosive threat detection technologies.

The DHS and DOD should collaborate on experimentation, testing, review, and standardization of technologies. To support these efforts, the DHS and DOD should form a joint forum at the assistant secretary level.

34. James Jay Carafano, Ph.D., "The Future of Anti-Terrorism Technologies," Heritage Foundation *Lecture* No. 885, June 6, 2005, at *www.heritage.org/Research/HomelandDefense/hl885.cfm*.

35. Marshall Billingslea, "Alliance Upgrade," *The Wall Street Journal Europe*, January 23, 2006.

36. For example, see Richard J. Aldrich, "Transatlantic Intelligence and Security Cooperation," *International Affairs*, Vol. 80. No. 4 (July 2004), pp. 731–753, and Brooks Tigner, "EU Officials Outline Obstacles to U.S. Trade," *Defense News*, May 30, 2005.

37. Billingslea, "Alliance Upgrade."

38. James Jay Carafano and David Heyman, eds., *DHS 2.0: Rethinking the Department of Homeland Security*, Heritage Foundation *Special Report* No. SR-02, December 13, 2004, p. 13, at *www.heritage.org/Research/HomelandDefense/sr02.cfm* (August 8, 2006). See also David Abshire, project chair, "Maximizing NATO for the War on Terror," Center for the Study of the Presidency, May 2005, p. 14, at *www.thepresidency.org/pubs/NatoReportMay05.pdf* (September 28, 2006).

39. Committee on Army Science and Technology for Homeland Defense—C4ISR, Board on Army Science and Technology, Division on Engineering and Physical Sciences, and National Research Council of the National Academies, *Army Science and Technology for Homeland Security: Report 2—C4ISR* (Washington, D.C.: National Academies Press, 2004), p. 41.

Internationally, the DHS should:

- **Use NATO.** NATO could use its Security Through Science program and Partnership for Peace Trust Funds more creatively to support homeland security technology R&D by EAPC members and Mediterranean Dialogue partners. Holding "reinforced" sessions of the North Atlantic Council and organizing informal special consultative groups among NATO experts and policymakers to address CEP initiatives could also bolster transatlantic collaboration in researching and developing homeland security technologies.[40]
- **Apply lessons learned.** The Technical Cooperation Program (TTCP) is an international organization that collaborates in defense scientific and technical information exchange and shared research activities for Australia, Canada, New Zealand, the United Kingdom, and the United States. It is one of the world's largest collaborative science and technology forums. The international community could apply many of the TTCP's practices to multinational S&T homeland security projects.[41]
- **Establish a clearinghouse.** Establishing a database of homeland security technologies is especially urgent. The DHS clearinghouse would describe existing technologies, their capabilities, and their possible missions. A technology clearinghouse would enable partners to know what technologies are available for transfer; provide a method of setting standards so that technologies are understandable; create a forum for interoperable and transferable means for industry-to-industry dialogue; establish predictable export control requirements; and construct acquisition mechanisms such as joint development programs, licensing agreements, and something comparable to the foreign military sales program.[42]
- **Consult with the State Department on proposed technology exports.** Congress should mandate consultations between the State Department and the DHS on proposed technology exports that have a significant homeland security purpose. U.S. export controls should distinguish among technologies that have a predominantly military, law enforcement, or homeland security application. The laws and regulations will also need to balance the benefits of sharing American homeland security technologies against the risks of foreign actors employing them either against U.S. defenses or for inappropriate commercial purposes. If a proposed technology transfer would promote the security of the United States and the recipient and is unlikely to be wrongfully acquired or used, the transfer should be governed by the Department of Commerce's Export Administration Regulations rather than by the more demanding provisions of the U.S. Munitions List, which are administered by the Directorate of Defense Trade Controls in the State Department.

The United States also needs either to broaden foreign involvement in the TSWG or to establish equivalent multilateral mechanisms for accessing the advanced technologies and innovative thinking found throughout the world. These efforts should extend beyond NATO cooperative initiatives to, for example, countries in South and East Asia.

The Way Forward

Ultimately, any real progress in strengthening global partnerships through sharing and jointly developing enhanced homeland security technology requires taking a hard look at duplicative investments and even whole programs. Pursuing this goal together with an investment strategy that reinforces itself would have a force multiplying effect. Improving international S&T cooperation will require investing the necessary funds, but cre-

40. Detailed proposals along these lines are presented in Abshire, "Maximizing NATO for the War on Terror."

41. For more information, see Technical Cooperation Program, "TTCP 101: A Beginner's Guide to the Technical Cooperation Program," February 8, 2006, at *www.dtic.mil/ttcp/TTCP101-8Feb2006.pdf* (August 8, 2006).

42. Carafano, "The Future of Anti-Terrorism Technologies."

ating a successful strategy will first require a substantial investment in careful thought.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. Jonah J. Czerwinski is Senior Research Associate and Director of Homeland Security Projects at the Center for the Study of the Presidency. Richard Weitz, Ph.D., is Senior Fellow and Associate Director of the Center for Future Security Strategies at the Hudson Institute.