Homeland Security: The Science and Technology Policy Challenge

24 February 2003

Integrated Summary of the
Symposium on Science, Technology and Security:
Knowledge for the Post 9/11 World
October 10-11, 2002
Boulder, CO

DRAFT FOR DISCUSSION

Organized by

Center for Science and Technology Policy Research
Cooperative Institute for Research in Environmental Sciences
University of Colorado

Sponsored by

University of Colorado - Boulder
University of Colorado - Colorado Springs
University of Colorado - Denver
University of Colorado Health Sciences Center
University of Colorado System
Rocky Mountain Institute for Biosecurity Research at Colorado State University
Graduate School of International Studies at Denver University
Alfred P. Sloan Foundation

Background

The security of the United States assumed a much greater importance in the wake of the tragic events of 9/11, and is captured with the phrase "homeland security." Scientific and technological knowledge and understanding are essential to enhance homeland security. Effective science and technology-based security policies depend critically upon assessing what knowledge is available, what knowledge is needed, and how decision makers might put that knowledge to effective use. In October2002 more than 60 scientists, scholars, and security experts spent two days at the University of Colorado at a Symposium entitled "Science, Technology and Security: Knowledge for the Post-9/11 World." Participants sought to foster new connections and thinking among the wealth of local experts on how better to integrate scientific and technological research with decision making on issues ranging from computer security to bioterrorism. The overarching goal of the Symposium was to recommend practical and effective strategies for improving the two-way connections between science and technology and security policy

- To consider challenges and opportunities for the practice of science and technology posed by the nation's enhanced focus on security policy;

- To consider challenges and opportunities for improving the connections of science and technology with the needs of decision makers;

- To consider alternative strategies for meeting the challenges and taking advantage of opportunities in the two way connections of science and technology and security policy;

- To consider the issues raised in the context of specific substantive areas: water, energy, information technology, critical infrastructure, bioterrorism;

- To produce a proceedings that summarizes the discussions at the Symposium and presents recommendations in support of the overarching goal.

The symposium brought together experts from Colorado and beyond in the physical, natural, and social sciences and the humanities to identify what we know, how to better use (and limit the misuse of) what we know, and what we need to learn, and to discuss issues and obstacles associated with each. The Symposium was sponsored by University of Colorado at Boulder, Colorado Springs, Denver and its Health Sciences Center, the University of Colorado System, Rocky Mountain Institute for Biosecurity Research at Colorado State University, the Graduate School of International Studies at Denver University and the Alfred P. Sloan Foundation.

Homeland Security: The Science and Technology Policy Challenge

Executive Summary

In October 2002 more than 60 scientists, scholars, and security experts primarily from the Colorado Front Range region spent two days at the University of Colorado at a Symposium entitled "Science, Technology and Security: Knowledge for the Post-9/11 World." Participants sought to foster new connections and thinking among the wealth of local experts on how better to integrate scientific and technological research with decision making in a diverse range of issues of homeland security. The overarching goal of the Symposium was to recommend practical and effective strategies for improving the two-way connections between science and technology and security policy. The Symposium focused on the application of these strategies in five substantive areas: information technology (IT) security, bioterrorism, water security, energy security, and critical infrastructure.

The Symposium was sponsored by University of Colorado at Boulder, Colorado Springs, Denver and its Health Sciences Center, the University of Colorado System, Rocky Mountain Institute for Biosecurity Research at Colorado State University, the Graduate School of International Studies at Denver University and the Alfred P. Sloan Foundation.

This executive summary provides an overview of the broad themes that emerged from the Symposium. The report concludes that successful policies related to homeland security will require new thinking, and most importantly, practical strategies for implementation of the nation's science and technology policies. As such, this report does not take on the task of prescribing particular research projects, but instead focuses on the broader challenge of improving the two-way connections between science and technology and security policy. The specific policy recommendations proposed in the five substantive breakout groups of the workshop can be found in the accompanying breakout group reports. The stakes are high. Failure to meet the challenge that homeland security poses for science and technology could lead to a less secure nation with profound implications for life and liberty.

The first broad theme is the interrelationship between strategic doctrine and science and technology policy. "Strategic doctrine" refers to the overarching policy framework that, in large degree, guides the foreign and domestic policies of the United States as they relate to our allies, enemies and others worldwide. As keynote speaker former Senator Gary Hart observed, globalization, information technology, the decline of the nation state (and, we might add, the rise of fundamentalism), change in the nature of conflict itself, and, of course, the tragic events of 9/11, all signify the need for a new strategic doctrine for American foreign policy. The Cold War strategic doctrine of "containment" largely determined the nation's overarching science and technology priorities for many years following World War II. Today, however, we may be on the cusp of a fundamental reordering of this relationship toward one in which science and technology continues to provide opportunity, but the limitations of science and technology dictate the parameters of practical, feasible, and effective strategic doctrine. Some factors warranting a rethinking of this relationship include the changing nature of threats to security and the increased access to all forms of science and technology, both dangerous and benign.

The second broad theme is that to understand the potential contributions of science and technology to homeland security, it is necessary to understand the scientific, technological and policy challenges of risk and vulnerability management. As used here "vulnerability" describes inherent characteristics of a system that create the potential for harm but are independent of the probabilistic “risk” of the occurrence of any particular event. A further distinction is between the “risk” of an event, say a terrorist biological attack on a major city, and the “risk” of a particular outcome, say 1,000 deaths in a terrorist attack.

The Bush administration’s proposed strategic doctrine of “preemption” focuses on risk management: identifying and dealing with the threat of an event before it results in adverse consequences. But history and research in areas as varied as natural hazards to engineering to domestic policy making suggest that “surprise” – resulting from an inability to anticipate every eventuality – is endemic to policy making. We should not expect the challenges of homeland security to be any different. A reality of security-related decision making is that in many cases accurate assessment of risk is simply impossible. Consequently, in cases where decisions are made based on inaccurate, incomplete or uncertain assessments of risk, risk management strategies could very easily result in outcomes quite different than those intended. The current strategic doctrine of preemptive does not distinguish vulnerability from risk. Alternative approaches to strategic doctrine may include an emphasis on enhancing resilience through vulnerability reduction (which itself may constitute a form of preemption).

Recommendations from the Symposium for the practice of science and technology common across the various substantive areas are expressed as three imperatives:

- increase collaboration,
- consider both dangerous and useful research, and
- learn and then apply lessons of experience in research and in practice.

The first recommendation emphasizes the importance of collaboration between traditional sectors (public and private), collaboration across levels of government (local, state, federal), and collaboration across disciplines, specifically with greater attention to the contributions from the humanities and social sciences. The second recommendation offers approaches for dealing with “dangerous” research that need not involve excessive government interference with academic freedom. It also focuses on the need for research to result in products and services that are of use to decision makers. The final recommendation recognizes that a range of experience in other contexts may provide useful information for thinking about and responding to the challenges of homeland security.

The formulation and application of an effective homeland security policy requires asking difficult questions that lie at the heart of science and technology policy – in the words of Congressman Sherwood Boehlert regarding creation of the Homeland Security department:

> Truth be told, I don't think anyone's yet even fully thought through the most basic question - in what ways do we want research related to homeland security to be different after this reorganization?

This report and accompanying documents reflect some initial efforts to think through that basic question.

Homeland Security: The Science and Technology Policy Challenge

Introduction

In the summer of 2002, the White House sent Congress proposed legislation to create a new Department of Homeland Security, noting, "in the war against terrorism, America's vast science and technology base provides us with a key advantage."[1] These remarks were echoed by the Chair of the House Science Committee, Congressman Sherwood Boehlert, "Our homeland security efforts will fail if R&D is not at their core." However, he also criticized the White House plan, "Truth be told, I don't think anyone's yet even fully thought through the most basic question - in what ways do we want research related to homeland security to be different after this reorganization?"[2]

This report, resulting from a fall 2002 symposium at the University of Colorado, takes on Congressman Boehlert's basic question. The report concludes that successful policies related to homeland security will require new thinking, and most importantly, practical strategies for implementation of the nation's science and technology policies. As such, this report does not take on the task of prescribing particular research projects, but instead focuses on the broader challenge of improving the two-way connections between science and technology and security policy. The stakes are high. Failure to meet this challenge could lead to a less secure nation with profound implications for life and liberty.

Successful homeland security demands a much closer linkage of science and technology and those who use the results of science and technology in preparing for and responding to security risks and vulnerabilities. An asymmetry in responsibilities exists as the vast majority of homeland security research activity comes from the federal government while homeland security decision making and implementation occurs in states, counties, cities and, most importantly, in the private sector. This factor alone suggests a need for a greater integration of "end users" into the processes of identifying and evaluating research priorities, and ultimately, turning the results of research into products and services that contribute to meeting the nation's homeland security goals.

The science and technology community has great experience in technology transfer, operational test-bed facilities, stakeholder involvement in research, research extension and so on. But to capitalize on such experience will require the learning of lessons and creating of new collaborations and connections between the federal government and the vast set of people and institutions with responsibility for homeland security. Meeting the challenge of making science and technology practical and relevant to homeland security will require experimentation, adaptability, and above all, a rethinking of the nation's Cold

[1] Office of Homeland Security, 2002. The National Strategy for Homeland Security, p. 52, http://www.whitehouse.gov/homeland/book/index.html

[2] http://www.house.gov/science/press/107/107-249.htm

War science and technology policies that have been in place largely unchanged since World War II.

Science and technology is a double-edged sword. It has a vast potential to contribute to the nation's homeland security goals, but at the same time those who seek to terrorize the nation look to science and technology as a means to exploit vulnerabilities, causing the exact harms the nation seeks to avoid. For example, when we teach students how to defend against computer-based security threats, we are also teaching them the skills they need to create these very threats, and thereby become successful criminals and terrorists. The same dynamic repeats itself in virtually all areas of science and technology.

Some argue convincingly that the general spirit of openness associated with research and education has led to innovation and contributed in no small way to the benefits of science and technology enjoyed by society. At the same time, few would deny the need to control access to nuclear, biological or chemical research that might facilitate the creation and deployment of weapons of mass destruction. Thus, homeland security also presents challenges for the practice of science and technology itself. How should we assess the trade-offs between closed and open approaches to research and education? What processes might be put into place to continually reassess such trade-offs as science and technology result in new discoveries? Such questions require careful study and considered attention if we are to effectively wield the double-edged sword to our benefit while avoiding potential harms.

Understanding the Big Picture:
The Interrelationship of Strategic Doctrine and Science and Technology Policy

We begin with a brief look at the big picture, the United States' overarching strategic doctrine and its interrelationship with the nation's science and technology policies. In his opening remarks at the Symposium, former Senator Gary Hart observed that because of September 11 "everything has changed."[3] He suggested that globalization, information technology, the decline of the nation state (and, we might add, the rise of fundamentalism), and change in the nature of conflict itself signifies the need for a new strategic doctrine for American foreign policy. To understand why we must begin to think differently about science and technology in the context of homeland security it is essential to understand the profound changes wrought by September 11 on the nation's approach to security, and this begins with consideration of "strategic doctrine."

"Strategic doctrine" refers to the overarching policy framework that, in large degree, guides the foreign and domestic policies of the United States as they relate to our allies, enemies and others worldwide. This framework has implications not only for the nation's military policies, but also its economic, social, humanitarian, and science and technology policies. The nation prospered for more than four decades during the Cold War under the strategic doctrine of "containment," focused on limiting the global expansion of the Soviet Union. With the end of the Cold War, "containment" gave way to "enlargement" focused on managing the consequences of the globalization of

[3] http://sciencepolicy.colorado.edu/events/security_symposium_2002/garyhart_speech.pdf

international economies. September 11 marked the end of "enlargement" as the United States' post-Cold War strategic doctrine. Its replacement is not yet agreed upon, though President George W. Bush has proposed a strategy of "preemption" – the identification and reduction of future risks -- as a candidate for the nation's post-9/11 strategic doctrine.

Whatever strategic doctrine the United States eventually settles upon will not only have profound consequences for science and technology, its success in implementation will depend critically upon science and technology. Gary Hart observed at the Symposium that September 11 has changed everything. One of the significant changes has been to elevate the role of science and technology as a factor that not only is affected by the choice of strategic doctrine, but also provides constraints on the choice of strategic doctrine. It is not an exaggeration to observe that after World War II, the United States' Cold War strategic doctrine of "containment" largely determined the nation's overarching science and technology priorities. This was possible because of the tremendous advances in knowledge and its application resulting from investments in science and technology.

Today, we may be on the cusp of a fundamental reordering of this relationship. The new relationship may be one in which science and technology continues to provide opportunity, but the realities of science and technology dictate the parameters of practical, feasible, and effective strategic doctrine. In the arms race that characterized the Cold War, containment was furthered by any and all advances in science and technology, so long as the United States made those advances before the Soviet Union. Today, the potential for certain scientific and technological advances gives pause to a strategy of following science and technology wherever it may lead. For example, difficult questions surround the issue of under what circumstances it would be beneficial to seek advances in the technology of weapons of mass destruction (e.g., nuclear, biological, chemical) or weapons of mass effect (e.g., "dirty" bombs, cyberterrorism, agricultural bioterrorism, etc.). Does the development of such technologies make the nation more or less secure?

One important factor motivating a rethinking of our approach to science and technology is the changing nature of the threats to security. The nation states that occupied the focus of attention in the Cold War have been displaced at the focus of geopolitical attention by decentralized terrorist organizations such as al Qaeda that have shown both the desire and capability to inflict great harm upon the citizens of the United States. Another important factor is what might be called the "leveling" of access to science and technology. Nuclear, biological, and chemical weapons are more attainable by groups seeking to inflict harm than at anytime in history. One of the central challenges of the nation's new focus on homeland security must be understanding and dealing with this broad access in the context of the many vulnerabilities of the interdependent water, power, computer and other systems that comprise the nation's critical infrastructure.

To understand the new focus on homeland security and its profound implications for science and technology policy, it is necessary to understand the evolving interrelationship of strategic doctrine and science and technology policies. There is a long tradition of considering the role of science and technology in foreign policies.[4] In 1970 Zbignew Brzezinski, who was later National Security Advisor to President Carter, wrote "the impact of science and technology on man and his society, especially in the more advanced countries of the world, is becoming the major source of contemporary change."[5] Under the doctrine of containment such change was not only manageable, but desired and encouraged through policy. Today, dealing with such change is one of the central challenges for the development of an effective homeland security policy.

Containment: Science and Technology Fuel the Arms Race

The Cold War policy of "containment" was first described in a 1947 article by George Kennan, in which he wrote "…it is clear that the main element of any United States policy toward the Soviet Union must be that of long-term, patient but firm and vigilant containment of Russian expansive tendencies."[6] Although Kennan's proposed containment policy referred to political and military containment, the Cold War was fought through an ever escalating arms race and regional conflict around the world, most notably in Korea and Vietnam, but in many other locations as well. In 1950, motivated by the Soviet Union's detonation of an atomic bomb, a National Security Council directive (NSC-68) characterized the military imperative, "Without superior aggregate military strength, in being readily mobilizable, a policy of 'containment'--which is in effect a policy of calculated and gradual coercion--is no more than a policy of bluff."[7] In order to achieve such military superiority, investments in science and technology to fuel the development of U.S. military power while keeping track of the Soviet Union's attempts to do the same became central to the Cold War.

For example, satellite technology alerted the United States to the positioning of missiles in Cuba in 1962, precipitating the Cuban Missile Crisis. In addition, the prospect of nuclear Armageddon, otherwise known as Mutually Assured Destruction or MAD, was thought to be central to containing Soviet expansion. Science and technology also had a central role in Cold War skirmishes fought off of the battlefield. The "space race" from the Soviet Union's launch of Sputnik, the first Earth-orbiting satellite, to Neil Armstrong's first small step onto the moon had everything to do with demonstrating international prestige and preeminence and the military applications of associated spin-offs technologies. Under containment, wherever science and technology took us is where we wanted to go.

[4] See, for instance, E. B. Skolnikoff, 1969. **Science, Technology and American Foreign Policy**, MIT Press, Cambridge, MA.

[5] Quoted in N. Wade, 1977. Breziniski: Role of Science in Society and Foreign Policy, *Science*:195:966-968.

[6] G. Kennan, (signed as X.) 1947. The Sources of Soviet Conduct, *The Atlantic Monthly* http://www.historyguide.org/europe/kennan.html

[7] http://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm cites as U.S. Department of State, *Foreign Relations of the United States: 1950*, Volume I. See also P. Y Hammond, 1962. NSC-68: Prologue to Rearmament, pp. 267-378 in Warner R. Schilling, Paul Y. Hammond, and Glenn Snyder, **Strategy, Politics, and Defense Budgets**, Columbia University Press.

Enlargement: Science and Technology as Tools of Multi-lateralism

In 1993 under the administration of President Bill Clinton, Anthony Lake, Assistant to the President for National Security Affairs, proposed that in the post-Cold War era "the successor to a doctrine of containment must be a strategy of enlargement -- enlargement of the world's free community of market democracies."[8] Enlargement, according to Lake, had four components: strengthening of developed market democracies, nurturing of new market democracies, liberalization of states hostile to market democracy, and advancing a humanitarian agenda.

Because enlargement focused on democracy and the global economy, science and technology (particularly in defense) no longer played the prominent role it had under the containment strategies of the Cold War. The reduced role for science and technology led to several calls by prominent scientists for a greater role in foreign policy.[9] Such calls were motivated, in part, by concern among scientists that changing strategic doctrine would alter the clear justification for the balance and size of research and development expenditures of the Cold War era. Timothy Wirth, Undersecretary for Global Affairs in the State Department under President Clinton described the evolving role of science and technology under a strategy of enlargement, "Science plays a critical role in our foreign policy by providing the foundation for our initiatives and negotiations on forests, chemicals, oceans, health, climate and many other issues."[10] Science, then, was to be a tool of multi-lateral engagement, representing a dramatic shift from the arms race-fueled strategies of the Cold War. Whatever the prospects were for Enlargement as strategic doctrine, as Gary Hart noted, 9/11 changed everything.

What Next? Preemption and the Devolution of Strategic Doctrine

Led by former Senators Gary Hart and Warren Rudman, the U.S. Commission on National Security of the Council on Foreign Relations issued a report in 2002 that noted three "facts of life" after September 11.[11]

- First, America is in a war with terrorists who want to attack its homeland, and it must act urgently to reduce its most serious vulnerabilities.
- Second, bolstering America's emergency preparedness in the near term is essential to minimizing casualties when an incident occurs on U.S. soil.

[8] The Clinton-era policy of "enlargement" as described here is based on the remarks of Anthony Lake, 1993. From Containment to Enlargement, September 21, Johns Hopkins University, http://www.mtholyoke.edu/acad/intrel/lakedoc.html An excellent resource for period documents on U.S. foreign policy is the home page of professor Vincent Ferraro at Mount Holyoke College, http://www.mtholyoke.edu/acad/intrel/feros-pg.htm

[9] See, e.g., Science and Technology in U.S. International Affairs, 1992. Carnegie Commission on Science, Technology and Government, New York, http://www.carnegie.org/sub/pubs/science_tech/internat.txt and J. Watkins, 1997. Science and technology in foreign affairs, *Science* 277:650.

[10] T. Wirth, 1997. Letter, *Science* 277:1185.

[11] G. Hart and W. Rudman, 2002. America Still Unprepared – America Still in Danger, Report of an Independent task Force, Sponsored by the Council on Foreign Relations.

- Third, America's own ill-prepared response can do more damage to its citizens than any single attack by a terrorist

"A proactive mindset is key … a reactive mindset is inevitably wasteful in terms of resources and can distract agencies from anticipating more probable future scenarios and undertaking protective measures."[12] A perspective of "preemption" was accepted by the administration of President George W. Bush as the next evolution of the nation's post-9/11 strategic doctrine.

In September 2002 President Bush announced the "National Security Strategy of the United States" observing,

> The gravest danger our Nation faces lies at the crossroads of radicalism and technology…. And, as a matter of common sense and self-defense, America will act against such emerging threats before they are fully formed. [13]

The document provides the following details of a doctrine of preemption:

> We will always proceed deliberately, weighing the consequences of our actions. To support preemptive options, we will:
>
> - build better, more integrated intelligence capabilities to provide timely, accurate information on threats, wherever they may emerge;
> - coordinate closely with allies to form a common assessment of the most dangerous threats; and
> - continue to transform our military forces to ensure our ability to conduct rapid and precise operations to achieve decisive results.
>
> The purpose of our actions will always be to eliminate a specific threat to the United States or our allies and friends. The reasons for our actions will be clear, the force measured, and the cause just.

If the United States' continuing efforts to disarm Iraq are the first invocation of preemption, then experience through February 2003 suggests that its viability as strategic doctrine remains very much in doubt. But irrespective of the outcomes of the U.S. conflict with Iraq, there are other reasons to question the efficacy of preemption as strategic doctrine, particularly as related to the challenges of homeland security and terrorism. These questions come not from ideology or partisanship, but from the practical realities of of using science and technology as means to address risks and vulnerabilities.

[12] Hart and Rudman 2002.

[13] http://www.whitehouse.gov/nsc/nss.pdf Additional documentation on the national security policies of the Bush administration can be found at : http://www.mtholyoke.edu/acad/intrel/bush/doctrine.htm

Homeland Security: Risk Management and Vulnerability Management

To understand the relationship between preemption and science and technology policies it is critical to distinguish between vulnerability-based and risk-based approaches to homeland security.[14] As used here the word "vulnerability" describes inherent characteristics of a system that create the potential for harm but are independent of the probabilistic "risk" of the occurrence of any particular event. A further distinction is between the "risk" of an event, say a terrorist biological attack on a major city, and the "risk" of a particular outcome, say 1,000 deaths in a terrorist attack. The latter definition of "risk" integrates both the characteristics of a system and the chance of the occurrence of an event that jointly result in losses. The point of this distinction is to consider homeland security from the perspectives of vulnerability and risk.

Preemption, as described in the section above in the experts from President Bush's National Security Strategy, is focused entirely on risk management: identifying and dealing with the threat of an event before it results in adverse consequences. But history and research in areas as varied as natural hazards to engineering to domestic policy making suggest that "surprise" – resulting from an inability to anticipate every eventuality – is endemic to policy making. We should not expect the challenges of homeland security to be any different. *The Economist*, in a survey on computer security, discusses the implications of this reality in the context of cyber-security.

> Total computer security is impossible. No matter how much money you spend on fancy technology, how many training courses your staff attend or how many consultants you employ, you will still be vulnerable. Spending more, and spending wisely, can reduce your exposure, but it can never eliminate it altogether. So how much money and time does it make sense to spend on security? And what is the best way to spend them? There are no simple answers.[15]

Questions of costs and benefits of alternative preemptive strategies are systemic across all areas of security policy. Raphael Perl, an expert on international affairs with the Congressional Research Service, points to the same set of questions at the international level, "the challenge to United States and European policymakers is to exercise such [preemptive] options wisely and to recognize which situations can be improved by use of preemptive action and which not."[16]

To understand the consequences of alternative courses of action requires an ability to accurately anticipate risks and project into the future the consequences of alternative actions to mitigate those risks. There is a large body of scholarship on methods of anticipation –called risk assessment, the process of determining the probabilities of

[14] For an elaboration on this discussion see Sarewitz, D. R. A. Pielke, Jr, and M. Keykyah,. 2003 (in press). Vulnerability and Risk: Some Thoughts From A Political and Policy Perspective, *Risk Analysis*.

[15] *The Economist*, 2002. A Survey of Digital Security, October 26.

[16] Terrorism and Foreign Policy, text of remarks given before the German Council on Foreign Relations, Berlin Germany, July 2, 2002. http://usinfo.state.gov/topical/pol/terror/02070204.htm

certain events – and mitigation of those risks – called risk management. Both approaches seek to accurately foretell certain future events and their consequences so that decision makers might have a more informed basis for selecting one possible course of action over another. However in cases where risk assessment is imprecise and risk management is uncertain, reliance on such strategies can in fact introduce pathologies to a decision process.

Consider the following examples and the challenges for security decision making raised by each:

- According to Charles Mann writing in the Atlantic Monthly, "to stop the rampant theft of expensive cars, manufacturers in the 1990s began to make ignitions very difficult to hot-wire. This reduced the likelihood that cars would be stolen from parking lots—but apparently contributed to the sudden appearance of a new and more dangerous crime, carjacking."[17]

- In April, 1997, in spite of a highly accurate forecast of record flooding made 2 months in advance, residents of Grand Forks, North Dakota evacuated from their homes in the dark of night as flood waters unexpectedly overtook the city. The NWS sought to communicate the severity of the situation by predicting a record flood of 49 ft. Residents interpreted the forecast to mean "don't worry" as the flood of record in 1979 was 48.8 feet.[18]

- In September, 1999, NASA's $125 million Mars Climate Orbiter burned up in the atmosphere of Mars after making a ten month trip. The loss occurred because one engineering team used metric units and another used English units. According to a NASA spokesman "The problem here was not the error, it was the failure of NASA's systems engineering, and the checks and balances in our processes to detect the error. That's why we lost the spacecraft."[19]

The examples highlight the challenges for policy making posed by unintended consequences, properly gauging and responding to information on risk, and errors introduced by decisions themselves. In light of such realities, the airline industry, for example, seeks to reduce the possibility of terrorist attacks not by seeking to anticipate particular attacks, but instead by seeking to manage its vulnerability through extensive screening of passengers and their luggage, irrespective of the true risks. Such a strategy is not necessarily inconsistent with the notion of preemption, but would require broadening present consideration of preemption to be inclusive of vulnerability-based approaches, as well as risk-based approaches.

[17] C. Mann, 2002. Homeland Insecurity, *The Atlantic Monthly*, September http://www.theatlantic.com/issues/2002/09/mann.htm

[18] Pielke, Jr., R.A., 1999: Who Decides? Forecasts and Responsibilities in the 1997 Red River Flood. *American Behaviorial Science Review* 7:83-101. http://sciencepolicy.colorado.edu/homepages/roger_pielke/hp_roger/pdf/1999.161.pdf

[19] http://www.cnn.com/TECH/space/9909/30/mars.metric/

Similarly, questions over the public accessibility of certain types of dangerous research, on techniques that would make smallpox or other diseases more virulent for example, are at their core questions about the trade-offs between risk and vulnerability. The trade off is between providing information that might be used by terrorists, thus increasing risk and lethality of attacks, and providing information which might be used by decision makers and the public to reduce their vulnerabilities to attacks.[20] And identification and management of "dangerous research" is itself a question of risk assessment and management.[21]

Questions about "dangerous research" are made complicated because many scientists view the open and unfettered exchange of information as a central tenet of the scientific process. Similarly, some argue that any limitations placed upon the flow of scientific information should be made by scientists alone. Ronald M. Atlas, president of the American Society for Microbiology, suggests that this issue "could change the very definition of science."[22] He observes that withholding certain data from publication is "not new to cryptographers and not new to physicists, but it's new to biologists, biologists have never seen this before."[23] Further, participants at the Symposium raised concerns that onerous or excessive restrictions on biological agents, on foreign students and scientists, or on publication of research results could well discourage competent scientists from working in critical areas. John Marburger, Science Advisor to President Bush, characterized the general problem, "I am somewhat concerned about overreactions, but we do need to be very clear about what kinds of practices and knowledge should be withheld from publication, and I don't think we have the final word on where to draw this line."[24]

A reality of security-related decision making is that in many cases accurate assessment of risk is simply impossible.[25] Consequently, in cases where decisions are made based on inaccurate, incomplete or uncertain assessments of risk, risk management strategies could very easily result in outcomes quite different than those intended. And, as Eugene Skolnikoff of MIT observed at the Symposium "our vulnerabilities are in an important sense endless, can be reduced but not eliminated, and can only be tackled over a long period of time."[26] Enormous resources could be devoted to vulnerability reduction rather than alternative and potentially more effective strategies. While vulnerability management is not inconsistent with a preemptive strategic doctrine, and is in many ways interwoven with risk assessment (what vulnerabilities? To what events?), discussion of

[20] For discussion, see R. Monastersky, 2002. Publish and perish, *The Chronicle of Higher Education*, October 11, p. A16 ff.

[21] For discussion see the articles in AAAS, 2003. *Science and Technology in a Vulnerable World*, Supplement to AAAS Science and Technology Yearbook 2003. American Association for the Advancement of Science, Washington, DC.

[22] Monastersky 2002.

[23] Schema, D. J. 2002. Sept. 11 Strikes at Labs' Doors, *New York Times*, 13 August.

[24] Schema, D. J. 2002. Sept. 11 Strikes at Labs' Doors, *New York Times*, 13 August.

[25] Some argue that historical trends in terrorist attacks, 9/11 included, do not justify dramatic policy shifts, see, e.g., R. Congleton, 2002. Terrorism, Interest Group Politics, and Public Policy, *The Independent Review*, 7:47-67.

[26] See, e.g., Lichtblau, E. Terror attacks on 'soft' targets complicates security, *New Your Times*, 30 November.

preemptive doctrine is incomplete because it does not distinguish vulnerability from risk. Bruce Schneier, CEO of Counterpane Internet Security, in his essay “how to think about security” integrates considerations of the costs and benefits of both risk and vulnerability management in five questions that he proposes asking of any security solution: What problem does the security measure solve? How well does the security measure solve the problem? What other security problems does the measure cause? What are the costs of the security measure? Given the answers to steps two through four, is the security measure worth the costs?[27]

Several Symposium participants suggested “resilience” as a guiding principle in vulnerability reduction efforts. While resilience was never precisely defined, elements include redundancy and standardization. Lewis Branscomb noted that the critical infrastructure on which we depend for our daily lives has become increasingly concentrated, more interdependent, and less redundant, as firms drive for greater efficiency, thereby increasing vulnerability. Symposium participants suggested that we might increase our resiliency and reduce our vulnerability by, for example, employing redundant electrical power grids in which the grid stays up even if it loses a large plant, and increasing our use of decentralized energy sources such as renewable energy and energy efficiency. University of Colorado professor and Symposium participant Ronald Brunner observed “The term might also help science (including science-based technology) in becoming more contextual and less reductionist, more iterative and adaptive and less linear, more inclusive of human factors, and so forth.”

Debate over homeland security has not yet focused on the implications of differentiating between risk and vulnerability, and the different roles played by science and technology under alternative approaches to security. An ability to distinguish situations that are more amenable to risk management from those that are more properly focused on vulnerability management, and the proper trade offs between the two, is a necessary precondition for the successful application of a preemptive approach to security.

The Science and Technology Policy Challenge: Recommendations and Next Steps

Participants at the Symposium included a wide range of scholars in academia and government (focused on Colorado institutions) as well as several practitioners whose jobs focus on the implementation of security policies in the public and private sectors. The recommendations of the Symposium fall into two general categories. The first are specific recommendations made by participants in breakout groups on bioterrorism, information technology, water, energy, and critical infrastructure. These specific recommendations can found in the accompanying reports from the Symposium breakout groups. The following recommendations from the Symposium were common across the various substantive areas.

[27] How to think about security, Bruce Schneier, Counterpane Internet Security, http://www.counterpane.com/crypto-gram-0204.html

The recommendations are expressed as three imperatives: increase collaboration, consider both dangerous and useful research, and learn and then apply lessons of experience in research and in practice.

Increase Collaboration

Several issues or concerns came up repeatedly in the Symposium. Perhaps the most common of these was the identification of a critical need for improved communication in many different settings: between technological and human systems, between producers of scientific research and those seeking to use the results of research, between government and the public, between and among official agencies, and so on. This subject is clearly important in this relatively new era of international terrorism for which a quite new set of actors is often involved. In many of the areas of identified need, the question is how knowledge can be effectively transferred from the laboratory to the field, from the government agency to the public, or from one agency used to working in one environment to another with a different environmental background and experience.

Collaborate across traditional sectors

A large portion of the nation's infrastructure is in the private sector. This creates a clear requirement for improving and expanding government/industry relations and for designing incentives and policies that will make possible effective industrial participation in the counter-terrorism effort. It is often not realized, especially when the demands pose seemingly different challenges from the past, how much experience there is on techniques for effective transfer of science and technology into the public and private sectors, and how much excellent literature and experience is available. We in fact know a great deal about how to engage in self-conscious design of new institutions (or new increments to old institutions) for S&T and security, but putting that knowledge into the right decision contexts is a challenge. It will be important to avoid re-inventing the wheel.

Lewis Branscomb observed at the Symposium,

> The historic discontinuities described by Gary Hart place stress on the ability of politics to adjust to the new realities. Issues like balancing freedom of inquiry and publication against constraints to limit diffusion of information to terrorists will be difficult for the political community to handle rationally. The fact that the Academies' study had to be financed by the Academies' own funds – and might well have faced questions about its publication had a government agency sponsored it – suggests that for some period of time more reliance will have to be placed on private initiative and resources.[28]

In an essay Branscomb highlights the critical role of the private sector:

[28] The study referred to was co-chaired by L. Branscomb: National Research Council, 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, p. 29, National Academy Press, Washington, DC.

> The key problem is that 85 percent of the critical infrastructure of the nation is owned by the private sector. Aside from public facilities in cities and national monuments like the Statue of Liberty, this infrastructure constitutes the terrorists' primary targets. Industry is waiting for government to decide who does what, who pays for it, and how a competitive economy can be maintained while reducing those elements that while adding efficiency create serious vulnerabilities.[29]

Symposium participants noted that Congress often sends inconsistent policy signals to industry, making it difficult for industry to plan infrastructure expenditures that might serve to reduce the vulnerabilities of critical infrastructure systems.

Collaborate across levels

Symposium participants noted that the science and technology-based military industrial complex that served us well in the Cold War will be of marginal value in the post-9/11 world. Lewis Branscomb argued, "the new threat is not war; it has no beginning and no end. Even the enemy is largely unknown…The government will try, but it will not protect us from the threat of catastrophic terrorism. It can only make the terrorists' job harder."

Gary Hart and Warren Rudman observe that in the context of homeland security "Federalism is an asset."[30] Most federal resources have been directed to federal efforts such as the development of the Department of Homeland Security. But there are several reasons for approaching the S&T issues in homeland security from the "bottom up." First, it is much easier to arrange collaboration among sectors – government, industry, universities and independent laboratories – at the local rather than federal level. Second, if all communities, counties, and states address the key vulnerabilities in their area, terrorists will have more difficulty assessing the feasibility of attacks than they might if the federal government centralized protection. Third, the emergency operations controls, the first responders, and the targets are essentially local – indeed at the level of counties and municipalities. Collaborating with local responders will help assure that the technologies developed for their use are appropriate, acceptable, and effective..

At the same time, states and localities frequently lack the resources to implement tools and techniques from existing scientific and technological research, much less any advances from new research and development. Thus, the federal government, constitutionally charged with providing for the common defense, will furnish the largest share of resources to confront the challenge of terrorism. Symposium participant David Guston of Rutgers University observes that these resources include the knowledge generated by federal investments in scientific research, particularly the three-fifths of all federal R&D expenditures provided to universities, government labs, university-operated

[29] L. Branscomb, 2002. Thoughts on catatrophic terrorism in America, *Ogmius: Newsletter of the Center for Science and Technology Policy Research*, Number 3, University of Colorado, Boulder, CO. http://sciencepolicy.colorado.edu/ogmius/archives/

[30] Hart and Rudman 2002.

Federally Funded Research and Development Centers, and other non-profit organizations. First responders and state and local decision makers, however, have knowledge about their informational, material, organizational, and technological needs that is not (and cannot be) anticipated by other, distant actors. So while the federal government is likely to remain the locus of funding for science and technology related to security, development of products and services that are actually used at the state and local level will require attention – and resources – from the federal level to the needs of decision makers in those settings.

An example of successful transfer of science and technology into the hands of local decision makers occurs in the context of agricultural production. Through agricultural extension, the knowledge generated by research conducted in land-grant universities is integrated with the competencies of farmers who have tacit knowledge about their particular situation that university scientists likely do not have. Agricultural extension is a process of active mediation and collaboration between traditionally conceived "knowledge producers" (university researchers) and "knowledge users" (farmers). The collaboration is based on local knowledge that the "users" possess, and thus the collaboration results in the "co-production" of knowledge-based innovations that benefits both parties. Researchers from land-grant institutions benefit from access to real data and opportunities and from seeing their research put into to practice. Farmers benefit from knowledge-based innovations that respond to their particular needs, and the mediators – extension agents – benefit from their successful facilitation of the co-production.

The century-long success of agricultural extension has more recently inspired the organization of manufacturing extension, in which the federal government teams up with states to provide local, knowledge-based assistance to small manufacturing enterprises. In a similar fashion, the federal government and states could team up to provide knowledge-based assistance to private and public institutions to enhance homeland security. A "Homeland Security Extension Service" would help connect traditional users of security services with innovators, making innovations more easily deployable through co-production of knowledge between the producers and consumers of science and technology and thereby improving the security of places of business, hospitals, universities, libraries, state and local government offices, and other institutions that might not be well-protected against moderately sophisticated terrorists.

A second recommendation would take further advantage of publicly supported knowledge resources, such as federal laboratories which exist in most states and have clearly defined missions to respond to national needs and to engage in technology transfer. A "Homeland Security Cooperative Exchange and Fellowship Program" would allow for greater interaction of knowledgeable individuals from federal labs and local and state governments. State public health officials, for example, could receive training in computer simulations at federal laboratories, and government scientists could be funded to gain experience working with local officials and first responders that would inform their research efforts. Such an arrangement would enhance the role of technology transfer – which includes transfer to state and local governments in addition to commercial entities – in the mission of the federal laboratories.

As an example of a practical application of this discussion, symposium participants noted that existing science and technology is sufficient to enhance the security of water supply and treatment facilities, but the connections between the science and technology community and the water sector are not particularly strong. These connections could be improved through small pilot projects responsive to specific local needs and which include robust dialogue, experimentation, and feedback mechanisms that permit progress to be made while learning from mistakes.

Collaborate across disciplines

The National Research Council's 2002 report on the role of science and technology in countering terrorism observed,

> Experts from many fields, including physical, biological, and mathematical sciences, engineering, and the social and behavioral sciences, stand ready to create new knowledge that, in turn, creates new capabilities. Science and engineers can put a powerful set of counter-terrorism tools at our disposal. But whether, when, where, and how we use these tools will be far from obvious and will require careful thought and analysis.[31]

Participants at the Symposium agreed that the nation's future research agenda must emphasize both the humanities and social sciences as keys to understanding the roots of terrorism and finding ways to make the world a more peaceful, free and economically healthy place. The participants recognized such undertaking as the only permanent answer to the threat of catastrophic terrorism and one that deserves a place within the nation's strategic doctrine. This echoes a recommendation of the President's Council of Advisors on Science and Technology,

> Terrorism is developing in a manner that cannot be approached entirely through devices, substances and information technology. The terrorist threat involves human behavior, culture, religion and differing world views, as well as behavior and motivations largely unfamiliar to most Americans. It can disrupt us by playing havoc with our economy, transportation, supply chains, legal system, and our psychology. Elements of DHS R&D should therefore involve social scientists, humanists, and "out of the box" thinkers from a wide variety of backgrounds. Highly unusual interdisciplinary work will be required. The R&D functions of DHS should operate so as to promote such non-conventional scientific collaboration.[32]

For example, a political scientist suggests that the events of September 11 should cause researchers in his discipline to rethink their intellectual priorities in "a useful new

[31] National Research Council, 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, p. 29, National Academy Press, Washington, DC.

[32] PCAST, 2002. Report on Maximizing the Contribution of Science and Technology Within the New Department of Homeland Security, 23 July, http://www.ostp.gov/PCAST/DHSreport.html

direction." He highlights the importance of research on decision making in the face of imperfect information, constraints on time and other resources, and untended consequences – or "bounded rationality" in the jargon of the field. He notes "governments and organizations, like people, can learn – especially when they have to. Political scientists, if they embrace the relevant interdisciplinary partners, can help."[33] This will confront universities with a funding problem, since few of the federal science support agencies have shown any inclination to invest in these areas. It also suggests that significant educational reform is needed, focused on a greater diversity of investments across multiple disciplines, as well as developing interdisciplinary research capabilities and skill in connecting research with the needs of decision makers.

Thoughtful consideration of both dangerous and useful research

Gary Hart noted in his keynote address to the Symposium that we face a step function in history, not a temporary change where it is likely we will return to the world as we knew it. Vulnerability to catastrophic terrorism will continue indefinitely, whether or not specific terrorists are captured or deterred. At the Symposium Eugene Skolnikoff offered a contrary perspective by suggesting that it would be easy to "get carried away with unrealistic efforts to harden America" and that we should "ensure that homeland security investments also contribute to the quality of life of civic society." This suggests that the governance of the research enterprise can be viewed from two perspectives: *dangerous research* which may increase risks or reduce vulnerability, and *useful research* that can be effectively incorporated into decision making to reduce risk or increase vulnerability.

The scientific community has considerable expertise with the conduct of secret or classified research, as well as research conducted in the private sector that is proprietary and not public. However, the post-9/11 concern with dangerous research raises concerns that regulations imposed on "sensitive but unclassified information" could easily be counterproductive if not designed carefully and implemented with understanding of the scientific research process and the value systems of universities, as well as the broader public interest in governing science and technology. Some traditional scientific and university procedures may require modification, for example, areas of information that were previously readily available may now have to be protected in some way. But important first-order questions are, Who decides? Under what processes? And who implements the new rules?

Government-imposed regulations implemented by national security agencies historically have often damaged rather than supported national security. It is critical that the scientific community show leadership on this issue, suggesting appropriate rules and implementation procedures that are reflective of the values essential to the vitality of the scientific enterprise as well as the counter-terrorism effort that is to serve society at large. If the community does not respond adequately, rules and procedures will be imposed upon the scientific community rather than designed in a collaborative process.

[33] Valelly, R. How political scientists can help fight the war on terrorism, *The Chronicle of Higher Education*, *The Chronicle Review* 19 July, p. B10.

Inquiries into security and vulnerabilities since September 11, such as the National Academy of Science report, have focused on how terrorists may turn knowledge against society. There have been proposals that faculty at individual institutions engage in security-motivated review of the research performed there for its possible appropriation by terrorists. The experience of human subjects research and research integrity, however, demonstrates that this type of institutional-based self-regulation does not work well enough without some federal oversight and coordination role. An alternative approach would be for the federal government to spur the creation of locally based offices for anti-terrorism technology assessment, roughly based on the current models of human subjects protection and research integrity. Local committees would not censor work, but they would advise researchers at any and all stages of their work about how to secure their laboratories and research materials and how best to communicate their research results without increasing the risk of misappropriation. They could also be a focus of decision making about whether or not to engage in high-risk research, e.g., recombinant DNA research with pathogens, and they could help identify research that could have potential terrorist applications.

As Eugene Skolnikoff observed, the sense of being "at war" carries significant dangers. It leads to an "excessive attention to the nation's vulnerabilities" and can produce a "panic atmosphere that we are facing immediate and grave risks that must be corrected at once." This sense of panic can lead to restrictions of civil liberties and scientific endeavors that are unwise and counterproductive, according to Skolnikoff. For example, some of the Symposium participants reported that the federal government's restriction of access to information about water system vulnerabilities has hindered local efforts to implement mitigation measures. Such restrictions on information flow also may inhibit technology transfer. Ultimately, in seeking to create useful research while addressing the potential for dangerous research will require the involvement of the public through mechanisms of democratic decision making to govern the scientific and technological enterprise.

Learn and then apply lessons and experience in research and in practice

Participants in the Symposium observed that there was a considerable amount of relevant, related experience in research and practice in fields such as natural hazards, nuclear weapons research and development, biotechnology and in the challenge of connecting research with decision makers. For example, according to Joeseph G. Perpich, a former official of the National Institutes of Health, the Recombinant DNA Advisory Committee (RAC), established in 1973, provides a model for the successful resolution of debate over potentially dangerous research.[34] Perpich summarizes three key elements of the approach taken by the RAC: establishment of research guidelines, public participation, and the creation of a federal interagency committee to discuss and evaluate a range of policy alternatives for consideration by decision makers. He further notes the importance of participation of individuals from the public and private sectors, as well as expertise from

[34] Perpich, J. G. 2002. The Recombinant-DNA Debate and Bioterrorism, *The Chronicle of Higher Education*, *The Chronicle Review* 15 March, p. B20.

science and bioethics. To avoid "reinventing the wheel" and to benefit from knowledge and experience gained in other contexts, it would be valuable for those focusing on homeland security to solicit input from others in relevant contexts.

One important lesson of experience identified by Symposium participants is the need for institutional flexibility and adaptability in the implementation of homeland security policies for science and technology. This is consistent with an observation of the President's Council of Advisors on Science and Technology:

> Management flexibility is of paramount importance in the initial organization of R&D programs within DHS -- in terms of organization, personnel and budget. Especially in this initial formative stage, and given that DHS must successfully merge existing programs and cultures, flexibility in organizing an overall structure and establishing operational programs will be vitally important. The management of technical programs is best conducted in an environment where requirements are clearly specified for the broad goals and objectives, but specific mandates and prohibitions regarding how to achieve these objectives are avoided.
>
> In establishing the R&D function, a long-term perspective must be maintained. Every decision need not, and indeed should not, be made immediately upon formation of the Department.
>
> As discussed at the end of this report, it is vitally important that DHS be an adaptive, highly flexible organization. Charged with defending the homeland from terrorist attacks, DHS will be a civilian agency operating in a demanding environment. Operations from existing agencies, which had very different missions, cannot govern the functioning of DHS. The Department must be allowed to establish a work ethic and culture that is new and different, and that remains fast-paced, responsive and current (especially in the R&D arena). The importance of allowing creativity to flourish cannot be overstated.

Radford Byerly noted at the Symposium that with respect to institutional design, members of the science and technology community have historically been "creationists" when what is needed today are "evolutionists." One of the most fundamental challenges facing the science and technology community in the pos-9/11 world is to institutionalize an adaptive, learning capacity in order to incorporate the lessons of unfolding experience and knowledge into homeland security policies.

Conclusion

In 2002 the President's Council of Advisors on Science and Technology characterized science and technology as a double-edged sword:

> Science and technology have created a fundamental change in society during the past half-century. For the first time in history, individuals or small groups can threaten the lives and livelihood of very large groups. This gives leverage to

> individuals who can "live among us" and wield terrorism as a weapon—even against a nation with near dominance in conventional conflicts on the land, at sea, in the air and in space. .. At the same time, science and technology (S&T) can be an even stronger weapon for countering terrorism—supporting such functions as sensing the presence of weapons, data mining, identifying individuals, communicating information, and the development of vaccines, to name but a few.[35]

This perspective is dramatically different than that espoused on June 17, 2001 in an article in the New York Times which asserted, "some experts believe that science's influence in public policy matters has not been at such a low ebb since before World War I."[36] September 11, 2001 changed many things in the world, and among them, a realization of the critical importance of science and technology policies.

Science and technology have great potential to contribute to the needs of those engaged in risk and vulnerability management in local, state and federal government agencies as well as in the private sector. At the same time understanding *what* science and *what* technology should contribute to *what* mix of risk and vulnerability management in *what* contexts under *what* mechanisms of democratic governance is the essence of the science and technology policy challenge posed by homeland security. Meeting the science and technology policy challenge will require increased collaboration among public and private sectors and levels of government, simultaneous consideration of both dangerous and useful research, and learning and then applying lessons learned in research and practice in an adaptive, evolutionary manner.

The challenge of homeland security for science and technology policy is intimately intertwined with the nation's strategic doctrine. Science and technology provide both the capacity for and limitations on preemption as the nation's national security stance. Any approach to preemption that is not grounded in the realities of science, engineering or politics could result in a decrease in security. An immediate need in consideration of preemption is to make room for the notion of "resilience," specifically the appropriate balance of risk management and vulnerability management as a means for implementing a preemptive doctrine. In achieving this balance, the formulation and application of an effective strategic doctrine requires asking difficult questions that lie at the heart of science and technology policy – in the words of Congressman Sherwood Boehlert appearing in the introduction to this report:

> Truth be told, I don't think anyone's yet even fully thought through the most basic question - in what ways do we want research related to homeland security to be different after this reorganization?[37]

[35] PCAST, 2002. Report on Maximizing the Contribution of Science and Technology Within the New Department of Homeland Security, 23 July, http://www.ostp.gov/PCAST/DHSreport.html

[36] Glantz, J. 2001. Sure, it's rocket science, but who needs scientists? *New York* Times 17 June.

[37] http://www.house.gov/science/press/107/107-249.htm

This report and accompanying documents reflect some initial efforts to think through that basic question.