Science and Technology in a Vulnerable World

Science and Technology in a Vulnerable World

Supplement to AAAS Science and Technology Policy Yearbook 2003

Albert H. Teich
Stephen D. Nelson
Stephen J. Lita
editors

Committee on Science, Engineering, and Public Policy

American Association for the Advancement of Science

The AAAS Board of Directors, in accordance with Association policy, has approved the publication of this work as a contribution to the understanding of an important area. Any interpretations and conclusions are those of the authors and do not necessarily represent views of the Board or the Council of the Association.

Printed in the United States of America

ISBN 0-87168-685-6

American Association for the Advancement of Science
1200 New York Avenue, NW, Washington, DC 20005 USA
www.aaas.org/spp

CONTENTS

PREFACE

As the largest general scientific society in the world, the American Association for the Advancement of Science (AAAS) has both the opportunity and the obligation to provide strong leadership for the science and technology (S&T) community, not only within science and engineering but in the relationships of science and technology to society. The Association's central mission is to ensure that the work of scientists and innovators continues to advance science while serving the needs of society. Throughout its 154-year history, AAAS—which draws its membership from all fields of science and engineering as well as from interested members of the lay public—has led the way in facilitating communication between scientists and policymakers, by analyzing critical issues, providing a forum for their discussion, and speaking out on such issues on behalf of the S&T community.

The September 11, 2001 terrorist attacks upon the United States make it imperative that the S&T community consider carefully the contributions that it can make to combating terrorism and strengthening homeland defense. At the same time we in this community must consider the impacts that strengthening security measures will have on the nation's research and education institutions. We must make sure that the conditions under which the United States has developed the world's most dynamic scientific and engineering enterprise are not jeopardized in the name of increased security, so that scientists and engineers can continue to conduct and communicate their work in ways that benefit the long-term public interest.

Security measures initiated by the federal government are already having impacts on many scientific institutions, including, especially, the nation's research universities. It is vital that all members of the S&T community carefully consider their own professional and personal roles and responsibilities in the post-September 11 environment. AAAS has expedited the publication of this book in an effort to bring these issues to the wider community of scientists, engineers, and policymakers, and to stimulate a broader dialogue concerning the responsible conduct and use of science and technology in the new era of security concerns.

The six chapters comprising *Science and Technology in a Vulnerable World* are based on talks presented at the AAAS Colloquium on Science and Technology Policy, April 11-12, 2002, in Washington, DC. The Colloquium, which has been held annually since 1976, provides a forum for discussion and debate about budget and policy issues facing the S&T community. Not surprisingly, the roles of S&T in the war on terrorism and homeland defense were highlighted at this year's meeting, and provided the theme: "Science and Technology in a Vulnerable World: Rethinking Our Roles."

In an ordinary year, these six Colloquium presentations, together with other papers from the meeting, and other key articles, speeches, and reports that appeared during the year, would have been published as part of the 2003 *AAAS Science and Technology Policy Yearbook*, which will appear in December. However, this is not an ordinary year, nor are this volume's issues ordinary policy concerns. Hence, we have decided to expedite their publication by producing this volume. The remaining Colloquium papers will be published on a regular schedule and both it and this book will be available online at www.aaas.org/spp/yearbook.

Science and Technology in a Vulnerable World begins with an article by M.R.C. Greenwood, chancellor of the University of California, Santa Cruz, and a past president of AAAS. Greenwood's paper, "Risky Business: Research Universities in the Post-September 11 Era," is based on the 2002 William D. Carey Award Lecture, which she presented at the Colloquium. In her chapter, Greenwood outlines the risks to research universities that may accompany proposed changes in policy stemming from the threat of terrorism and proposes approaches for addressing these risks.

Chapter 2, by Lewis M. Branscomb, Aetna Professor of Public Policy and Corporate Management emeritus and former director of the Science, Technology and Public Policy Program at Harvard University's Kennedy School of Government, and co-chair of the National Academy of Sciences' Committee on Science and Technology for Countering Terrorism, discusses the changing relationship between science and government in recent months, and the role that science and technology play in both enabling and countering terrorism.

Donald A. Henderson, principal science advisor to the Secretary of Health and Human Services for public health preparedness and chairman of the Secretary's Council on Public Health Preparedness,

contributed Chapter 3. Henderson focuses on the dangers posed by bioterrorism, discusses the steps the government is taking to prevent future attacks, and provides a brief overview of the problems faced by the research community.

A paper on the national information infrastructure by Eugene H. Spafford, professor of computer science and philosophy, and director of the Center for Education and Research in Information Assurance and Security at Purdue University, comprises Chapter 4. In it, Spafford outlines some information security problems the nation faces, including the increasing number of computer viruses, poorly written software, and a shortage of professionals in computing science.

In Chapter 5, Baruch Fischhoff, university professor in the Department of Social and Decision Sciences and the Department of Engineering and Public Policy at Carnegie Mellon University, examines the psychology of risk, risk analysis, and risk communication, and applies our growing understanding of these areas to the problems posed by the threat of terrorism.

The book concludes with a paper by Eugene P. Skolnikoff, professor of political science emeritus at the Massachusetts Institute of Technology. Skolnikoff discusses the impacts that the events of September 11 have had on research universities, and whether the responses required by future threats conflict with the values that universities embody in the course of their work.

AAAS hopes that the papers in this volume will contribute to the public discussion of how science and technology can contribute to the war on terrorism and homeland defense while preserving their essential values of freedom and openness. As always, we would be pleased to receive comments and suggestions from readers on this book and on how we might pursue these objectives most effectively.

Albert H. Teich
Stephen D. Nelson
Stephen J. Lita

Washington, DC
July 2002

1 Risky Business: Research Universities in the Post-September 11 Era

M.R.C. Greenwood

On September 11, 2001, the nation was attacked. We knew deep in our hearts that the world was changing before our eyes; that the freedoms and openness we had taken for granted were now being used against us; and that our lives—both personal and professional—would never be the same.[1]

As members of the research science and technology (S&T) community, we knew that we would have a key role to play in ensuring the future safety of our country. But sometimes in our community we forget that the research university is first and foremost a "university" and not just a scientific or technological institute where new knowledge about the natural world is generated and processed into new products. The word "university" is derived from the Latin root *universitas*, meaning "whole" or "body," yet we often forget the whole and work in departmentalized, segmented units. We must keep in mind the whole university, as we will need the full complement of intellectual tools within those institutions to ensure our national security and well being.

The Opportunity and Danger before Us

The following poem was brought to my attention by Wlad Godzich, the dean of humanities at the University of California, Santa

---

M.R.C. Greenwood is chancellor of the University of California, Santa Cruz. *This chapter is based the William D. Carey Award Lecture delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy, held April 11-12, 2002, in Washington, DC.*

Cruz, and himself a scholar of the role of the humanities in an era of globalization and technology.

> The time will come, America,
> When the hordes of Afghanistan
> Will crash your gleaming airplanes
> Into the shiny towers of Manhattan.
>
> —*Surrealist Revolution* (1925)[2]

These words are shocking and prophetic. They were not, however, based on any military, technological, or scientific analysis of our national security. They represented the views of some creative impressionists of that era who harbored no love for an America they saw as materialist, imperialist, and sterile.

It is not surprising that in this early period of our nation's response to terrorism, we are focusing on bolstering national security to guard us from future attacks. Our government's efforts to protect the nation are starting to unfold in many aspects of our lives, most markedly in airports. But policy changes are occurring in other arenas too, and this chapter discusses some of those policy changes that are potentially risky business for research universities in the post-September 11 era.

All of us are uncomfortable with changes being forced on us by outside actors who are not under our control. But now is not the time for the science and technology community to engage in days of "whine and poses." With crisis and change come tremendous opportunities. I am reminded of the Chinese symbol for crisis, which is a combination of the symbols for danger and opportunity. Facing up to our new dangers and opportunities will require the best of America, and the best of those of us at research universities. We, like most Americans, want to be part of advancing national security in all of its forms.

What do I mean by national security in all of its forms? I mean security from

- biological and chemical warfare;
- nuclear and radiological threats;
- systemic damage to information technology, computers, and telecommunications;
- assaults on our transportation system, energy facilities, buildings, and fixed infrastructure;
- slipping into economic turmoil; and, most importantly,
- the failure to understand the roots of terrorism.

The public and our policymakers may need to be reminded that research universities play a unique role in all of these areas. Our universities educate and train students who will become the next generation of informed and engaged citizens, as well as the scholars in all disciplines, the professionals and leaders in all fields, and of course, the scientists and engineers who will help us face these tremendous challenges.

We must, therefore, reach out to our colleagues in academe and our fellow citizens in government, indeed to our entire society, to forge a new compact to work together. Research universities now have a once-in-a-generation opportunity to renew and redefine a partnership (a compact, if you will) with the federal government to develop new programs, new areas of research, and new strategies to advance our national security and improve our society.

It is understandable that since September 11, there has been a close hold on information, and that strategic decisions have been made under the auspices of the military, as well as intelligence and law enforcement agencies. But, as we move from reaction to action to proaction, new ways to work together must be developed.

Research Universities in the Post-September 11 Era

Leading a public research university since September 11 has been an illuminating and transforming experience on many levels. My conviction is even stronger now than it was then that the universities can and must play a critical role in understanding and preventing terrorism in the next generation. As much as I have been inspired by the contributions of our scientists and engineers and the bravery of our firefighters, police, and medical personnel, I also have been struck by how much we can learn from our research colleagues in the social sciences and the humanities in bringing about a deeper understanding of the interconnectedness of our world. We saw this demonstrated at the University of California, Santa Cruz, when our faculty organized and engaged in a variety of forums with students, the community, and local religious leaders. These gatherings offered perspective on the rise of terrorism and the clash between modernity and fundamentalism.

As one would expect, the research S&T community immediately began to make significant contributions to our safety and well being. In short, many of us found ourselves involved, in small and large ways, as "civic scientists engaged in civic duty."[3] For example:

- Experimental robots developed at the University of South Florida helped in the search-and-rescue efforts at the World Trade Center towers. The robots showed how leading edge technology could be applied immediately to search in areas that were too dangerous for humans.

- During the Olympics, biosensors developed at the Lawrence Livermore and Los Alamos National Laboratories were used to help detect the presence of hazardous biological agents.

- Technologies to detect explosives are being used extensively in airports around the nation, as well as in the subways of Washington, DC. Some of these technologies were developed by those same national laboratories.

The Risks in the Proposed Changes in S&T Policy

I will elaborate on the importance of the whole university below, but first, I want to go back to the risky business of proposed changes in S&T policy and their potential impacts on research universities. The proposed changes relate directly to our changed threat level and perceived risk as a nation. History shows us that perceived risks change our national security policy, and always have. But these changes are, I believe, risky business for research universities.

Let me focus on three specific risks:

- proposed limitations on researchers' access to data and methodologies;
- proposed allocation of tax dollars in the Administration's FY 2003 budget, in particular the changing allocation of research and development (R&D) with an increased emphasis on "missiles and medicine"; and
- the move to increase the tracking of foreign students in universities.

Risk 1: Proposed limitations on researchers' access to data and methodologies

The basic issue with the first proposal is the shift from the "right to know" to the "need to know," which threatens to erode some basic democratic principles, as well as the basic framework of scientific interactions.

Balancing the perceived risks of open access with the risks to the health and vitality of the research community is exactly the kind of issue that calls for a new partnership between the research community and the government.

The news media have reported that in its initial attempts to assess the threat of terrorists developing harmful chemical, biological, or other agents of mass destruction, the Office of Homeland Security has expressed an interest in requesting, or requiring, limitations in

scientific publishing, especially in publishing data sets and methodologies that might lead to replicating certain results.[4, 5] The risks and benefits of such actions must be clearly understood. The tradition and structure of research in the United States today depend on replication and refutation. This means that sufficient data and methods that allow for sufficient data must be published in peer-reviewed journals.

Openness has enabled the vast majority of advances in civilian applications and innovations in the last 50 or more years, and makes our research system the envy of the world. It has led to new knowledge, and thus innovations that drive our economy, ensure national security, and fight terrorism. It also militates against fraudulent results, sloppy science, and political biases guiding important policy decisions. In addition, open communication of results influences our national policies in environmental and health issues. We cannot imagine environmental or health policies that are not based on the open access and review of research data.

A recent example from *Science* illustrates this point. Scientists reported to have seen evidence of nuclear fusion in a beaker of organic solvent. Much controversy accompanied the publication of this paper, referred to as "bubble fusion," but *Science's* editor-in-chief Donald Kennedy argued (correctly, in my view) that publication is always the right option, even when there is controversy. He said:

> …that's what we do; our mission is to put interesting, potentially important science into public view after ensuring its quality as best as we possibly can. After that, efforts at repetition and reinterpretation can take place out in the open. That's where it belongs, not in an alternative universe in which anonymity prevails, rumor leaks out, and facts stay inside.[6]

Of course, some circumstances may warrant restrictions, but the onus for blocking publication should be on the government through a process that is clearly defined, free of arbitrary edicts, and understood by the research community. This is exactly the kind of issue that calls for a new kind of partnership between the government and research universities.

History can inform us about how to engage with our government in meaningful ways in helping to set national science policy that maintains and strengthens the science and technology research enterprise. Through much of our national security history, but especially since World War II, national security priorities have had a strong influence on national science policy. They always have and they always will. The events of September 11 represent the beginning of yet another era of great change in our national security priorities.

To put my comments in context, it is necessary to reflect on the links between national security and national science policy during five eras of great change.

World War II

During World War II, scientists, engineers, mathematicians, and language specialists used their expertise to help fight the war. They made key contributions to the aviation industry; dramatically improved manufacturing, communications, and transportation systems; improved the health and nutrition of soldiers; developed new weapons; and used their mathematical and language skills to break codes, providing intelligence and enabling communication with resistance fighters in occupied countries. In addition, the government mobilized the physics and technology community to develop the first atomic bomb, which ended a world war.

But during this period of threats to the nation, our nation always expected that the war itself was an episode that would have an end and would someday be over. This expectation stands in contrast to our current war on terrorism, which President Bush has reminded us time and again will be fought using many different strategies on many different fronts for an unpredictable period of time. Furthermore, the current war is partly in our homeland. A major challenge is to be sure we understand the differences between homeland security and national security, especially when the objectives may be the same.

The Cold War

The very weapons that ended World War II opened a new era of national security, one focused on the proliferation of such weapons. When the Cold War started, the government mobilized scientists and engineers to work on defense R&D to ensure national security, which was defined primarily in the military terms of preparedness and deterrence. The goal was to keep the Soviet Union in check.

In the post-World War II era, Vannevar Bush's *Science—The Endless Frontier* defined nondefense R&D. As Bush stated in that report, "Scientific progress is one essential key to our security as a nation, to our better health, to more jobs, to a higher standard of living, and to our cultural progress."[7] This persuasive viewpoint laid the foundation for the rise of the American research university and the primacy of unfettered basic, or fundamental, research from the 1950s through the 1990s. This research was a driving force for innovation and growth in both civilian and defense R&D.

We began to see more clearly the links between research and development, or between doing research and then doing something with it. We also saw the links between fundamental research and advances in technology, and then how those advances in technology enabled more fundamental research. Thus, we witnessed the emergence of research and development as a network of enabling interactions instead of a linear progression.

Sputnik

In October 1957, a new threat, the launch of Sputnik, was a symbolic event that caused a shift in perceived risk. Changes in national science and technology policy followed. Beating the Soviets in space added to the patriotic fervor, and shocked us out of a sense of complacency derived from our economic successes of the 1950s.

End of the Cold War/*Science in the National Interest*

The fall of the Berlin Wall in November 1989 was another symbolic act that signaled the rapid end of the Cold War. Our national priorities changed once again.

In the face of a perceived reduced risk, our government leaders started to talk about a "peace dividend." Resources that had been devoted to national security, which had been defined primarily in military terms, would now be released for other uses. We began to think about broader ways to use our science and technology talents to advance our own national interests and those of our global partners.

Science in the National Interest, published by the White House Office of Science and Technology Policy in 1994, crystallized that way of thinking. It began to change the nature of the discussion. We went from characterizing R&D as defense R&D and nondefense R&D to speaking about R&D for broader national interests. National security was expanded to include economic security, environmental security, health security, and personal security with the following core elements:

- health security through understanding, preventing, and treating disease and ensuring an adequate, safe, and nutritious food supply;

- economic security and prosperity through technical innovation driven by basic scientific and engineering research, which in turn brings about technology improvements and revolutionary advances that create new industries;

- national security based on technological superiority bred of scientific and engineering innovation and a strategic commitment to both breadth and excellence in basic research;

- environmental security and responsibility that requires better understanding of the complex interrelationship among components of the biosphere, human activities, and the world around us;

- personal security, as demonstrated through improved quality of life through culture, inspiration, and full participation in the democratic process.[8]

Throughout the 1990s, industry, universities, and government made the case that fundamental research and innovations were creating entire new fields of economic activity. Whole new industries emerged, such as those that converted the Internet from a military network into a major public institution and force for economic growth and information exchange. Whole new classes of pharmaceuticals that resulted from biomedical research entered the market, such as the hepatitis B vaccine and protease inhibitors to treat HIV. And new commercial technologies, such as the global positioning system, are now in standard use in automobiles.

In the 1990s, the argument in support of science in the national interest seemed to capture people's imaginations. Perhaps most successful was "health security" and the advances in the life sciences. One measure of the nation's interest is the rapid increase in funding for the National Institutes of Health (NIH). Although personal health will always have the most general appeal, the science and technology and business communities were succeeding in the argument that strong health sciences also need the physical sciences and mathematics to continue to progress.

During the same time, the nation (including research universities) backed away from supporting the humanities, the arts, and the social sciences. Research universities, which were making a strong case for the support of science and technology and the role of industry, no longer were making the case for *universitas*. This is reflected in the fact that the entire budget request in fiscal year 2003 for the National Endowment for the Humanities is $127 million, and few U.S. students were studying foreign languages seriously. The severity of this issue was dramatically noted when Federal Bureau of Investigation (FBI) Director Robert S. Mueller III, at a press conference shortly after September 11, put the FBI's telephone number on the television screen in an attempt to recruit Americans who spoke Arabic, since we had a shortage of Arabic speakers.

Post-September 11

Our nation's scientists have traditionally stepped up to the plate when needed to work toward national goals, and clearly this has already begun. Over 125 of our nation's distinguished science and

technology experts have volunteered and are working together, through a committee of The National Academies, to develop a research agenda for countering terrorism. No one who has been asked to serve, including me, has declined the invitation. Our committee's report will be out in June, and I am confident that it will provide valuable advice for the nation.

Science in our nation, as the late Congressman George Brown, Jr. often reminded us, is funded through the political process. If we are to receive taxpayers' dollars, we must be seen to be responsive to perceived and real threats. It has been this way since the beginning of our nation.

Risk 2: Proposed allocation of tax dollars in the Administration's FY 2003 budget, in particular the changing allocation of R&D with an increased emphasis on "missiles and medicine"

I want to focus on a few significant aspects of the overall federal R&D budget, especially the emphasis on "missiles and medicine," and their impact on research universities.

- Today, defense and health R&D make up more than three-quarters of the federal R&D portfolio (which totals $112 billion in FY 2003), with both areas increasing.

- Research universities perform about 11 percent of the nation's total R&D, and with that share, do more than half of federally funded fundamental research.

- The federal government funds nearly 60 percent of the R&D performed by universities, but this percentage is going down.

- NIH funds nearly two-thirds of federal R&D at colleges and universities, a reality that strongly influences the mix of science and engineering disciplines in their R&D portfolios.

- Other disciplines such as engineering and the physical sciences now account for far smaller shares of the total academic R&D than in past years. Engineering gets 15 percent and the physical sciences get 9 percent of the total university R&D portfolio.[9]

These kinds of imbalances may mean that we might not be training the right mix of scientists, engineers, and other scholars that we will need to work for national security in the next generation. This is not to say that we need less funding for health R&D; rather, we need more nondefense R&D in many other disciplines. Perhaps it is even time for the science and technology community to help out its other colleagues and call for increases in federal funding for specific areas in the humanities.

While a "missiles and medicine" approach is predictable and a basically simple start on a counterterrorism agenda, it is only a beginning. A comprehensive agenda will require investments in many other research areas and a better balance to encourage new ideas. Already those of us on various counterterrorism committees are struggling with this dilemma.

I cannot predict how the rapid shifts in funding priority may directly affect our economy or our national security in the short term. But I can predict that any dramatic decreases in funding for some areas and resulting imbalances of research across disciplines are likely to have negative effects on the kind of research done in universities, as well as the training of scientists and engineers. Such redistribution needs to be carefully considered.

There is no question that the S&T community must provide leadership in research areas that lead to threat reduction. A new partnership between the government and research universities could identify important and significant foci for research and innovation. We need to develop forums and engage in serious discussions with our government leaders to make the case for carefully considered research priorities. By working together, we can avoid pouring money and people into some areas simply because things *can* be done, while we miss defining what *needs* to be done.

Risk 3: The move to increase the tracking of foreign students in universities

Our government is concerned that potential terrorists may abuse our student-visa process as a way to enter our country. As a consequence, the Homeland Security Presidential Directive-2 says:

> The Government shall implement measures to end the abuse of student visas and prohibit certain international students from receiving education and training in sensitive areas, including areas of study with direct application to the development and use of weapons of mass destruction.[10]

According to the U.S. Department of State, the "sensitive areas" could include:

- nuclear technology,
- missile technology,
- navigation and guidance control,
- chemical and biotechnology engineering,
- remote imaging and reconnaissance,
- advance computer/microelectronic technology,
- materials technology,
- information security,
- lasers and directed energy systems,
- sensors,
- marine technology,
- robotics,
- advanced ceramics, and
- high-performance metals and alloys.[11]

I cannot vouch for other universities, but a large portion of this list describes the University of California's research and graduate education portfolio in science and technology.

If implemented without careful consideration, this policy will be risky to our national security for many reasons. Three are given below.

- At least since World War II, the United States has prided itself on being a magnet for the brightest students from around the world who see our educational system as a beacon of hope. After studying in our universities, many stay and make significant contributions to our economy. Indeed, our newly nominated NIH director, Dr. Elias Zerhouni, is a perfect example of the kind of talent that comes to our country for training and opportunity, and then stays to serve our country. Andrew S. Grove, a founder of Intel, is another example. Others return and make positive contributions to their home countries.

- The United States benefits from the infusion of non-U.S. scientists and engineers by gaining access to valuable skills and by exploiting the development of new knowledge overseas.

- Moreover, restricting international students would contribute to an international perception that we are isolationist and imperialistic. That would not be a good thing for national security.

The National Science Board recently released the newest data regarding foreign-born scientists and engineers in the United States. The Board found the following:

- Significant numbers of scientists and engineers in the United States were foreign born. These include
  ? 9.9 percent of bachelor's degrees,
  ? 19.9 percent of master's degrees, and
  ? 27 percent of doctorates.[12]

- Foreign-born Ph.D.s make up
  ? 45 percent of the total U.S. pool n engineering,
  ? 46 percent of computer sciences, and
  ? 31 percent of mathematics.[13]

This foreign-born pool of science and technology talent is distributed across academe, industry, and all levels of government. In aca-

deme, for example, foreign-born Ph.D. holders comprise 28 percent of scientists and engineers.[14]

Our leaders have recognized that something must be done to better ensure that holders of student visas are actually studying in educational institutions, and partnerships are starting to emerge. After some initial difficulties, the higher education community responded positively and worked closely with Senator Dianne Feinstein (D-CA) and other public officials to address the vulnerabilities in our nation's student-visa program. The higher education community is now meeting regularly with the Immigration and Naturalization Service, which is implementing the Student and Exchange Visitor Information System.

However, if we perceive that the risk of abuse of our visa system is so high that we have to restrict foreign students, that decision will make sense only if we can also develop a policy that secures our supply of scientists and engineers in the future. A major issue for our nation is that our native-born students either are not sufficiently interested or are not being inspired to pursue science and engineering degrees. If we block access to foreign students, who is going to do the research of the future, and who will be our faculty of the future? This is a serious question that will impact directly on our long-term national economic security. If universities are restricted in their opportunities to attract students from other countries, we must increase incentives for U.S. students to study science, engineering, and mathematics. Again, working in partnership with our government, we must consider our options and develop new policies to manage this serious risk to our future national security.

There can and should be more such interactions with governmental leaders to reach solutions that serve national needs. If the United States decides to restrict access to foreign students, we would have to develop new policies *now* to prevent a net loss of science and engineering personnel at all levels in the next generation.

Proposal for Action

To that end, I propose a contemporary version of the National Defense Education Act (NDEA)—with a twist. It would be responsive to the current challenges we face.

NDEA was a direct result of an increase in the perceived risk to national security by the launch of Sputnik. It marked a change in national science policy in response to emerging national security concerns. The Act increased support for large numbers of students who became scientists and engineers from the late 1950s through the 1970s. One result was a rise in Ph.D.s awarded annually by U.S. colleges and universities from 8,600 in 1957 to 34,000 in 1973.[15]

In fact, I was a beneficiary of NDEA. Many scientific careers were launched in part, or in whole, because of policies that were put in place as the result of this Act. We need a new version of this program, designed with current challenges in mind, which will yield comparable results.

There may, however, be an even more compelling reason for a new federal initiative to draw U.S. students into science and engineering. Our homeland defense and national security needs should motivate us to tap into the large pool of women and minorities who have so far been underrepresented in science and engineering. Some critics of the research university argue that our encouragement of foreign students to populate our graduate and research programs is a result of our nation's unwillingness to provide significant incentives to our own young people, especially women and minorities, to get serious about science and technology careers. They argue that as a nation, and as research universities, we are unwilling to spend the needed resources to prepare, recruit, and then support all kinds of students to pursue these careers.

A contemporary federal initiative could finally tap into that huge sector of the population that has not been readily welcomed before. And a call to our young people from our government would be consistent with the President's call for national service. It would draw our most talented young people from all sectors of society to explore areas of scholarship that are important to national security, including all fields of science and technology and some fields in the social sciences and the humanities.

All sectors of our society, including science and technology, security and intelligence, defense, foreign relations, and economic development, need well-educated students in these areas for the future. This is, therefore, yet another important area that should be discussed

within the framework of a new partnership between government and research universities.

Need for a New Partnership

With discussion of these three risks, I hope I have been convincing that a new partnership is needed to work on viable solutions to the great challenges that face us.

I am reminded of H.L. Mencken's famous quote: "For every complex problem, there is a solution that is simple, neat, and wrong."

I propose instead that we pull smart, committed people together into new partnerships to develop solutions that are simple, straightforward, and *right*. That means a new partnership involving the research community working with public officials to make wise and fully informed choices now to ensure our national security in the long term.

Research Universities Reconsidered

I alluded to a major issue above that I would like to conclude with. Research universities have another critically important role to play in the immediate future that is not discussed nearly enough in the S&T community. That role is to help our nation better understand the complex social and cultural forces that are changing our world. In Karen Armstrong's book *The Battle for God*, she reflects on the struggle between modernity and fundamentalism in many religions and notes, "All over the globe, people have been struggling with these new conditions and have been forced to reassess their religious traditions, which were designed for an entirely different type of society."[16] We face this difficult struggle today, and will continue to face it for a long time to come. We must try to understand it and to help the next generation.

In short, there are many scholars in our universities who can help us to understand some of these issues as the first step of many steps toward finding some solutions.

These will be among the great challenges for the next generation of research universities. We can excel in science and technology, and

the education of scientists and engineers. And we can excel in preparing humanists and social scientists. But that is not enough. If we do no more than that, then the age-old two-cultures war will rage on at a time when the stakes are simply too high for disciplinary isolation. We must have a broader education to help all of us understand the complexity of the world around us. Perhaps reaching across the disciplines is one of the greatest challenges for the research university.

What will define a well-educated student and scholar in the next generation? Let me return to one of our scientific colleagues, E.O. Wilson, and his assertion in *Consilience: The Unity of Knowledge*:

> Every college student should be able to answer the following question: What is the relation between science and the humanities, and how important is it for human welfare? Most of the issues that vex humanity daily—economic conflict, arms escalation, overpopulation, abortion, environment, poverty—cannot be solved without integrating knowledge from the natural sciences with that of the social sciences and humanities. Only fluency across the boundaries will provide a clear view of the world as it really is…[17]

Preparing this truly well educated student is our most risky business in the next generation, and we must step up to the challenge now.

The scientific and technological creativity and innovation that support our national security in so many ways—economic, military, health, environment, education—will advance:

- if our research priorities are broad enough to enable exploration and discovery into new areas from which unanticipated benefits may be derived,

- if the free flow of information is not restricted without considerable deliberation and acknowledgement of risks to the overall R&D effort, and

- if we create pathways for our own students as well as the brightest foreign students to study and succeed in our research universities.

I am convinced that our universities have much to offer in this new globally oriented world of ours. I call on our community and our government to work together to address these new challenges constructively. If we do not, we will become a weaker country, and we will have allowed the terrorists to progress. If we are able to work together in ways that are respectful of each other's needs and strengths, we will emerge as a much stronger country, as well as a much better country.

Endnotes

1. The author wishes to thank Donna Gerardi Riordan for her substantial assistance in preparing this lecture.
2. Translated by Wlad Godzich, dean of humanities, University of California, Santa Cruz, April 2002.
3. M.R.C. Greenwood and Donna Gerardi Riordan. "Civic Scientist/Civic Duty." *Science Communication*, Vol. 23, No. 1, September 2001, pp. 28-40.
4. William J. Broad. "A Nation Challenged: Domestic Security; U.S. is Tightening Rules on Keeping Scientific Secrets." *The New York Times*. February 17, 2001.
5. *The Economist*. Academic Freedom: Secrets and Lives." March 9. 2002. pp. 75-77.
6. Donald Kennedy. "To Publish or Not to Publish." *Science*, Vol. 295, No. 5561, March 8, 2002, p. 1793.
7. Quote from Philip Kitcher. 2001. *Science, Truth and Democracy*. New York: Oxford University Press. p. 138.
8. White House Office of Science and Technology Policy, National Science and Technology Council. *Science in the National Interest*. August 1994.
9. Source of 2003 federal budget data: *AAAS Report XXVII: Research and Development FY 2003*.
10. George W. Bush. Homeland Security Presidential Directive-2. October 29, 2001.
11. U.S. Department of State. Visas Mantis (http://travel.state.gov/reciprocity/Mantis_TAL.htm)
12. National Science Board. *Science and Engineering Indicators 2002*. p. 3-29.
13. *Ibid.* p. 3-30.
14. *Ibid.* p. 5-24.
15. National Opinion Research Center. *Doctoral Recipients from United States Universities, 2001*. http://www.norc.uchicago.edu/issues/docdata.htm

16. Karen Armstrong. *The Battle for God.* New York: Alfred A. Knopf, 2000, p. xiv.
17. Edward O. Wilson. *Consilience: The Unity of Knowledge.* New York: Alfred A. Knopf, 1998, p. 13.

2 The Changing Relationship between Science and Government Post-September 11

Lewis M. Branscomb

The events of September 11, 2001 came as a great shock to the American people. But the anticipation of that day goes back a long time. Exactly 25 years ago Harvard professor Gerald Holton published a very interesting paper about terrorism[1] (it will be republished in 2002).[2] This paper describes three kinds of terrorism. Type I is traditional terrorism by an individual or small group of people who are determined to wreak havoc for reasons of their own. It is not connected with any government. Type II terrorism is conducted by a dysfunctional state, unable to deal with the rest of the world through normal interstate relationships. This state engages in terrorism either against its own people or against others. Type III terrorism occurs when the Type I terrorist (a stateless terrorist group) finds that it can get resources and technical support from a Type II terrorist state.

We now face Type III terrorism. We must understand that the source of our vulnerability to terrorism is not the terrorists themselves. Our vulnerability is generated by our economic, social, and political systems. Our vulnerability comes about through something I call economic ecology. This idea holds that competition in the

---

Lewis M. Branscomb is the Aetna professor of public policy and corporate management emeritus and former director of the Science, Technology and Public Policy Program in the Center for Science and International Affairs at Harvard University's Kennedy School of Government. *This chapter is based on remarks delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy held April 11-12, 2002, in Washington, DC.*

market economy maximizes efficiency and stability at the cost of resiliency. Economic ecology was the subject of the National Academy of Sciences (NAS) Bicentenary presentation to the International Council of Scientific Unions in 1976. It was a project of the Academy. A group of us, under my chairmanship, pointed out that through all of history, society has used science and technology (S&T) to try to increase efficiency and produce stability in the life around us. These two principles work fine, but they do so at the expense of resiliency, a well-known ecological principle that also works in economics. If you have a highly competitive market economy, everyone is driven to greater efficiency. But the public also wants stability. Stability, with only small perturbations, is built into the system. But this does not work unless you have a peaceful, obedient society that does not threaten to exploit these vulnerabilities. This society cannot avoid threats to leverage that very hyper-efficiency.

University-Government Relationships

University-government relationships have changed with every major war. Before and during World War II, and even for some time after, everyone understood that you dropped what you were doing when your country needed you. The science and technology community was totally dedicated to defeating the enemy, which was known and identifiable. Everyone pulled together in the expectation of unconditional surrender by the enemy. The war would have an end point, after which there would be peaceful life and civil society again.

The Cold War was somewhat different, in that it was of indefinite duration. But it was similar because the opponent was a state, which was well-known and well-recognized. We produced an unresilient (but effective) strategy called mutually assured destruction (MAD). The military and foreign policy people had the responsibility to manage that problem. Society had to support it, but it did not really upset our civil life. The military-industrial complex ran the "war." Academic support was primarily through the basic research agencies (such as the Office of Naval Research, the Air Force Office of Scientific Research, the Army Research Office, and the Defense Advanced Research Projects Agency).

The war on terrorism is different. We have an unknown enemy in our midst, and the duration is indefinite. We are creating vulnerabilities all the time. Unless we do something different, it is going to get worse.

The universities need to support the nation in this war, building on their traditional values. But we need some significant changes. Catastrophic terrorism is the ultimate in asymmetric warfare. We depended on S&T to compensate for the asymmetry in the Cold War, when Soviet forces greatly outnumbered ours. We compensated by having our forces technically superior. But, now, each terrorist threat is in some ways a new war. Terrorists are technically competent and may be armed with weapons of mass destruction. To what extent can S&T compensate for this asymmetry? What is the role of and the effect on the universities?

The first thing the universities realized is that the United States government is not structured to deal with a problem that does not fit in standard compartments. Is this war or is this crime? Is this a domestic problem or is this a foreign problem? Is this a short-term issue or a long-term issue? Is it the government's responsibility or is it the citizens' and the private sector's responsibility? Our government is structured so that it deals with every one of those pairs with two different sets of institutions and two sets of policies. The challenge of terrorism mixes every one of those two things together. It supremely challenges the structure and capability of not only the federal government but also its relationships with municipalities, states, and the private sector.

The U.S. technical community is ready to be called on. When NAS president Bruce Alberts called people to form the parent committee of a 24-person effort at NAS, every single person he called said yes. They all attended a meeting two weeks later. This country is ready to work on countering terrorism. The problem is how to do it. The question is whether the government is organized to benefit from what the universities can contribute.

Countering Terrorism

There are three ways to counter terrorism. One, you can reduce the incentives that create and motivate terrorists. This approach clearly falls in the category of foreign and military policies, international relations and alliances, and intelligence. S&T can certainly contribute here, through technical means and gathering intelligence and through social science studies. The ideal solution would be to make this a peaceful world in which the number of individuals willing to kill themselves to destroy societies was greatly reduced. But that is very hard to do.

Another way is to detect and arrest the terrorists. This is essentially a police function. This may be the cheapest of the three, but it is the one that bears most heavily on civil rights and civil liberties.

The third way is to harden the target society, that is, make it more difficult for the terrorists to attack. We do this by detecting their preparations, intercepting their plans, making the targets less vulnerable, limiting the damage they can do, and enhancing the recovery. Industry has a role to play in this area. But we must motivate industry to reduce the vulnerabilities inherent in our society.

The Nature of the Vulnerabilities

We credit science and technology not only for creating an efficient economy, but also for creating the weapons that terrorists use. These weapons are based on the same technologies we use domestically for beneficial purposes. Our S&T strategy to address this has to be very sophisticated. It has to use the very S&T that creates the vulnerabilities to lessen those vulnerabilities.

One of our biggest problems is that the critical elements of our infrastructure are deeply linked. When one part is attacked, we see a domino effect on the other parts. The three most obvious infrastructure elements are energy, communications, and transportation. If you bring down any one of these three, the other two are affected. For example, if you bring the energy sector down, you cannot communicate and you cannot travel. There is a lot you cannot do. Terrorists understand that, and we must deal with this reality. We have to con-

sider the threat of multiple, simultaneous attacks on our infrastructure.

Another problem was brought on by deregulation, by getting the federal government out of the markets. Over the last decade, we have introduced more competition, particularly in the energy area, by deregulating. One result of that is a significant increase in vulnerability.

The threats are now more varied than simply the weapons of mass destruction. They include bioterrorism, chemical warfare, nuclear attack, and radiation contamination. All of these threats affect infrastructure issues. They come together in the cities where people are, because people are the targets. In cities we face the key issue of managing the warnings of an attack, as well as the attack itself. We also have to support the first responders.

And, finally, of course, our defense has to address the issues of intelligence and borders. One of the unfortunate characteristics of almost every feature of security and defense, whether security against crime or against minor acts of terrorism, is based on a single, thin wall. We try to check people coming into the country, but once they are legally in, they are in. We can put a fence around a critical facility, but if you can overcome it, you are in. That is characteristic of most of our systems, even in the computer area. Computer security has the same thin wall, and it does not work. We need a lot of technical tools to address this. They include sensor systems, data systems and networks, biomedical vaccines, chemical warfare treatments, and biometrics for efficient identification. Some of these involve cross-cutting issues and human factors-decision systems.

Terrorism, to a greater degree than any problem before, calls for a new way of thinking about the nature of the threats and how to deal with them. It calls for systems engineering and analysis. It calls for strategy-driven goals for the research program and the creation of new capabilities. Basic research will help us develop the strategy we need. It will not give us the answers to the current problem, but it will tell us how to change the questions.

Basic Research

Basic research, if it removes ignorance in critical areas, can give us a whole new way to approach this problem and make it easier to solve. That, in my view, is the critical role of basic research. But when you think about it, the government is not well-structured to do anything that is built on a systems strategy that cuts across all the current missions and areas of technical activity in the country. Countering terrorism is going to touch on every discipline in the universities, not just technical areas. Importantly, this time we have to pay attention to what the social sciences and humanities have to contribute.

Many different fields will need to address the many requirements of the war on terrorism. Developing sensors and dealing with hazardous materials will involve chemistry, physics, and engineering. Nuclear and radiological threats will be addressed by nuclear science. Bioterrorism will need the biomedical sciences and medical services. Threats against energy will be on the agenda of the physical facilities themselves, their infrastructure links, engineering, and information technology. Transportation and distribution are in the realm of engineering. Protecting our water, food, and agriculture will need people from biology and chemistry. Cyberattacks will be met by information science and engineering. Cities and people will be protected by the social and behavioral sciences. Infrastructure linkages will be taken care of by systems analysis and systems engineering people.

The political world has always been skeptical about the contributions of the social sciences and humanities. There are areas of which social science cannot give actionable advice, but there are many other areas where it absolutely can. Social scientists have studied the terrorism problem in great detail and have things to tell us that are very important.

R&D Capability and Mobilization

The big difficulty is that the government and the universities are "stovepiped," with different areas in technical work segregated into different organizations; financed by specific agencies. In the government, we do not have to create an S&T capability. We have fabu-

lous S&T capability. It is nurtured by agencies born out of World War II and the Cold War. These agencies have massive capability to mobilize American science and technology. They are well-known: the National Institutes of Health, the National Science Foundation, the U.S. Departments of Energy (DOE), Defense and the National Aeronautics and Space Administration. These are big organizations devoted to a technical enterprise. But they do not, with the possible exception of the Department of Defense and some of DOE, have the mission of domestic security against terrorism. That mission is in agencies like the Federal Emergency Management Agency, the U.S. Customs Service, the Immigration and Naturalization Service, the U.S. Coast Guard, and the U.S. Department of Transportation. The latter is a technical agency, but it has never had a very strong research and development (R&D) capability. There are many other agencies, as well as state and local governments, in this situation. So the customers for science and technology are agencies with very little R&D experience.

Most of the U.S. R&D capability is in the hands of agencies that do not have the mission of countering terrorism. So how can we put all that together? When you go to the universities to get work done in physics, you know where to go. But if you want to solve a more complex problem, the universities are not internally structured, in most cases, to work on it. The implementation of any strategy depends on the federal government, which is capable of deploying most of the nation's capability (except that in the private sector).

We do not want to disrupt the present S&T capability. Instead, we are going to have to create an architecture for defining not only a strategy for using S&T in counterterrorism and managing its execution, but we also have to help the President manage that process. This requires linked-systems approaches and intersectional collaboration (involving the federal government, states, cities, and industry). It will be a challenge. We are not very experienced in this area. But most counterterrorism research must be interdisciplinary and in a systems context. We have our work cut out for us. As I said above, government science agencies tend to be stovepiped. Interdisciplinary work is hard to peer review. But many counterterrorism problems cut across agency lines. The university structure is also poorly adapted to a systems context and multidisciplinary work. We may

need some institutional innovations, both in government and in the universities.

The universities have many resources. They have research capability for creating new options and competencies. They have links to local government and industry. They have access to students and colleagues around the world. And they have relevant capability in the social sciences and humanities. But the universities have needs too. They need more research resources. They need to continue to have access to foreign resources and students, the freedom to share technical information, and acceptable levels of security. They need to be able to admit students and collaborate with foreign scientists without irrational restrictions. And they need to be able to handle and deal with the very difficult and unclear question of how sensitive information should be handled in the research community.

Possible Effects of a New Strategy

Positive effects could come out of all this. (Eugene Skolnikoff addresses the other side—the risks and threats to the universities—in Chapter 6 of this volume.) Important agencies of the government may learn how to use the research capacity of the country. We could also broaden the base of support, with new sources and levels of funding. We have seen a small trend over recent years in which the mission agencies do less and give the work to the National Institutes of Health (NIH), which, fortunately, has the money. But they also give work to the National Science Foundation (NSF), which does not have enough.

Second, an indirect consequence may well be some rebalancing of the disciplinary unbalance. We should not do this by reducing NIH. It needs generous funding because bioterrorism is so important. We should rebalance by adding funding for research in the physical sciences and engineering. This should help DOE, NSF, and other agencies to rebalance some of the disciplinary unbalance that we have all worried about. We may also see improved government ability to manage crosscutting research programs. If they do not improve in this area, we will have trouble working against terrorism. Importantly, we are going to have to learn how to develop more construc-

tive linkages with industry and state and local governments in ways the federal government has found hard to do in the past.

Third, the right research strategy will benefit "dual use" technologies. We can define problems to address civil as well as security needs. For example, we could develop better ways to detect an infection prior to seeing clinical symptoms. We can also develop ways to make needed capabilities affordable. New probes and sensors that identify and track containers reduce costs in time and money in normal commercial shipping. This has wide application. We can also find new ways to deal with natural disasters. This would include advancements in communications, robotics, and even clothing for firefighters and hazardous materials specialists. We could also improve threat characterization for first responders.

Finally, this new strategy may make education a new national priority. We are already seeing in Congress a renewal of interest in science and engineering education. The Technology Talent Act of 2002 has been introduced in Congress and Congress has been receptive. It seeks to increase U.S. student interest in science. Maybe out of this will come a 21st century version of the National Defense Education Act (as M.R.C. Greenwood suggests in Chapter 1). If we face a reduction in foreign students for any reason, the shortage of Americans going into science and engineering will only get worse. Bringing more American students into science and improving public education is a necessity. If we cannot tap a more diverse student body, which should include women and minority students, there is no way we are going to do it. We must improve the pipeline of the K-12 science education system. Demand for publicly financed R&D will stress current human resources in S&T. Congressional pressure on non-U.S. students (regrettable but likely) could strengthen the case for improved U.S. education efforts. We need to generate practical ideas that will actually work.

The good news is that basic research may emerge out of this to be seen as a strategic necessity. We may see a new balance between the physical and health sciences. Because the problem is so ill defined, we need an open-ended, imaginative, creative way of thinking about it. This will only come out of the basic research community, which has been substantially funded by the traditional civilian agencies (NSF, NIH, DOE, etc.).

The bad news is that as agencies re-label a large part of their programs as counterterrorism, they invite constraints. The research may be the same, but it may now be labeled as defending the country, and, therefore, critically important to national security. So Congress, knowing that the universities are so important, may put constraints on communication, publication, and the like, beyond what ought to be done. Legislation and agency policy may place information restrictions on grants. Indeed, counterterrorism is a preempting budget priority. So if you cannot re-label your program as counterterrorism, then that part of your budget may suffer. I hope this will not be the case.

We must look seriously at the government's inability to manage crosscutting research programs. Counterterrorism requires a systems approach. The systems approach demands capability at the top level of government to develop national research programs. This will help with maximizing interdisciplinary research, but it is going to put additional burdens on the White House Office of Science and Technology Policy, the Office of Homeland Security, and others. But it is very important that we have a strong, visionary capability to lead the definition of how S&T can help in this area. If successful, we can apply this approach to sustainable development, climate change, and other areas that challenge our quality of life.

Control of Information

The control of sensitive information is a big issue. This is a quote from *The Economist*, which I think is very perceptive.

> Knowledge is power. Those who possess it have always sought to deny it to their enemies…. But exactly what knowledge needs to be controlled depends on who those enemies are. Nor is the control of knowledge without cost.
>
> A free society should regard it as a last resort. Scientists cannot build on each other's results if they do not know them. And governments are frequently tempted to hide not only what is dangerous, but also what is embarrassing. That can result in dangers of its own.[3]

Unfortunately, the present state of government controls on information is chaotic. The system of military secret classification is not adapted to the terrorist threat. The U.S. Department of Health and Human Services has no legal authority to classify information as "secret." This means that information that could be extraordinarily dangerous if it were publicly known to the terrorists is not protected. We have to protect this information in some way until the rules are worked out as to how this will be done routinely. The term "sensitive but unclassified" is likely to be applied to much university work, even though it has no clear definition. We see serious, legitimate dilemmas about what should, in fact, be published. Add to this the Patriot Act (PL 107-56), which authorizes intrusion into the Internet, servers, answering machines, and other telecommunication equipment. (It also requires colleges to turn over student records, and requires the National Center for Education Statistics to turn over data in response to a warrant.)

This poses the question, but it does not give the answer, of how this will be done. Ultimately, we need to resolve a lot of open issues with respect to the government's view of sensitive information.

Security and intelligence on university campuses is a much more difficult problem now than during the Cold War. Public interest in security lapses at universities, real or imagined, will be intense. Terrorist threats are extraordinarily diverse and of indefinite duration. The public will expect research universities to track students who may be perceived as threats.

Conclusion

I think the scientific community is going to have to engage in a long debate. It should have started before September 11 because this debate has to do with things besides terrorism. It has to do with the moral and ethical responsibility of individual scientists and engineers. We all must think about how they can relate our activity in science, our communication, and all the things we do in a way that we believe benefits the long-term public interest.

Must the culture of science evolve to discourage its misuse? If so, in what ways? Is there a consensus on the expectations scientists place on themselves now? I believe that thoughtful self-constraint is

the only way to maintain the creativity of science and still protect the country.

Endnotes

1. Gerald Holton. "Reflections on Modern Terrorism." *Bulletin of the Atomic Scientists*, 32 (November 1976), pp. 8-9. [MS-628].
2. In Barbara Probst Soloman and Julie Berman, eds. *The Reading Room*, Great Marsh Press, NY. 2002.
3. Secrets and lives. 2002. *The Economist*, March 9.

3 Public Health Preparedness

Donald A. Henderson

Terrorism poses a set of unique problems in the civilian sector, problems we have not faced before. But these problems also offer a number of opportunities. I see both the problems and the opportunities in my role as director of the new Office of Public Health Preparedness in the U.S. Department of Health and Human Services. This office did not even exist six months ago. Yet we are charged with addressing some of the most critical challenges we have ever faced as a nation. Perhaps the most serious problem we must confront is the threat of biological weapons. In 1993, now Secretary of State Colin Powell said, "Of all the weapons of mass destruction, it's the biological weapons that worry me the most." As recently as March 28, 2002, U.S. Department of Defense Secretary Donald Rumsfeld said, "Terrorists and terrorist organizations want to acquire weapons of mass destruction, but I am primarily concerned about them getting and using biological weapons." In post-September 11 America, when we have already seen an outbreak of anthrax in our mail, these words carry even more weight.

We have long lived with the threat of nuclear war. But nuclear weapons are more difficult to handle, manage, transport, and detonate than are chemical or biological weapons. The latter offer new opportunities to terrorist groups and smaller nations. These weapons can be made in relatively small places, with dual-use equipment, and at a relatively low cost. And they have a variety of delivery mechanisms. Despite knowing this, we have done very little about dealing

---

Donald A. Henderson was director of the U.S. Office of Public Health Preparedness from November 2001 to April 2002. He served in that role while in leave from his position as distinguished service professor at Johns Hopkins University. *This chapter is based on remarks delivered at the AAAS Colloquium on Science and Technology Policy held April 11-12, 2002, in Washington, DC.*

with the threat of biological weapons until less than a year ago. We need to understand why we have not acted, because this delay has set in place our research agenda.

This chapter describes some previous incidents that have heightened our awareness, discusses the steps we are taking and where we are right now, and gives a brief overview of the problems ahead, particularly in the research area.

Previous Incidents and Response

We were not all that concerned about terrorism until 1995. During that year, three events happened that put the threat of biological and chemical weapons into sharp focus. The first was Aum Shinrikyo's attack in the Tokyo subway with sarin gas. In March, members of this group carried six packages onto the subway and then pierced them with umbrella tips. This released the deadly sarin gas, killing 12 and injuring 5,000. It was later discovered that they had tried on eight different occasions to aerosolize anthrax throughout Tokyo.

The second event was the defection of two of Saddam Hussein's sons-in-law in August. They brought with them chilling information about Iraq's advances in developing weapons of mass destruction. We found out that the sophistication and extent of the weapons in Iraq were far greater than we had thought, even though we had considerable intelligence in the area. We had to wonder what else was going on in the world, particularly in places where we had virtually no intelligence. We became concerned that there might be much more going on out there than we had imagined.

The third event actually happened in 1992, the information provided was not widely circulated until 1995. In December 1992, Ken Alibek defected from the Soviet Union. He was the number two man in their bioweapons program. He brought with him a fantastic tale of an enterprise then involving as many as 60,000 people in more than 50 different laboratories, dealing explicitly with biological weapons. This enterprise was equivalent to, and maybe slightly larger than, their nuclear enterprise. This information was regarded as being so outlandish that Abilek was kept under deep cover for quite a while. The information did not begin to be widely known until 1995,

when a Presidential directive to all departments mandated them to prepare to deal with terrorism.

In 1996, the Nunn-Lugar-Domenici Domestic Preparedness Initiative was proposed. It began a program that developed metropolitan medical strike teams, as they were called, in 120 cities in the United States. Police, fire, and emergency management personnel were trained, primarily through a program largely run by the Department of Defense.

During the course of this training, the term "chembio" arose because it was thought that if we have trained the first responders to deal with a chemical incident, they will also be able to deal with a biological incident. This idea has been surprisingly widely held throughout Congress and in the executive branch for quite a while, and it still revives regularly. In a chemical event or an explosive event, police, fire, and emergency rescue people are indeed needed to stabilize, evacuate, and decontaminate the area. But a biologic event is most likely going to be a silent, odorless, tasteless, undetectable release of an aerosol over an area. No one will know that anything has happened. Only after a couple of days to a couple of weeks do cases begin to show up in emergency rooms. The police, fire, and emergency rescue people are totally irrelevant to this problem. We would need trained medical personnel to counter a bioterrorism event through detection, patient treatment and perhaps isolation and the distribution of drugs or vaccines.

Are we addressing this need? In 1998, I spoke at a national conference on urban bioterrorism. There were probably 500 people in the audience. I asked if there were any physicians. Not one hand went up. Likewise, there was no one from public health, no one from a hospital, no one who had ever dealt with an epidemic. Attendees were police, fire, and emergency medical people, arms control people, physicists, mathematicians, and computer specialists. There was no one who had a clue as to what we were talking about when we discussed the use of biological weapons and the aftermath. It was not until 1999, that the budget for the Department of Health and Human Services, which has dealt with epidemics, was increased from $2 million to a $343 million. This increase allowed at least a beginning to do something to address this problem.

Historically, in the schools of medicine and public health, doing anything with biological or chemical weapons was virtually a taboo. When I was the dean at Johns Hopkins University for 14 years, we regularly turned down non-classified contracts from Aberdeen Proving Grounds that addressed physiologic behavior of various chemical agents related to nerve toxins. Indeed, anyone who had attended classified conferences was generally regarded with suspicion. It was a carryover, in part, from the Vietnam era. But there was also a feeling that those engaged in the healing arts should not have anything to do with chemical or biological weapons. This was not true in all universities, but it certainly was true in a lot.

Because of these attitudes, our research base is now very limited. We have identified many organisms of concern, but have very few people working on them. In fact, during an outbreak of plague in Surat, India, we hoped we would be able to contribute diagnostic capability. But so I was told, only one person (who was about to retire) was working in the United States on the laboratory diagnosis of plague.

Steps We Are Now Taking

We are in the early stages of thinking about what it is that we might do with regard to bioterrorism. We are oriented toward taking immediate steps to harden the civilian setting.

Our academic and research base is very small, indeed. This has to change. The Centers for Disease Control and Prevention identified six diseases to go on the Group A list. These are the diseases on which we want to focus to see what we can do in an immediate sense to cope with an attack. We are not concerned with a list of 30 or 50 diseases. We are concerned with a comparatively short list of diseases that would be catastrophic and potentially destabilizing. They are smallpox, anthrax, plague, tularemia, botulinum toxin, and the group of diseases that manifest themselves as hemorrhagic fevers. Of these, smallpox and anthrax are the most important.

How do we expect these to be released? We considered all of the possible mechanisms and identified the aerosol spread as the one we are most concerned about. Contaminating food or water is possible but unlikely to result in a potentially destabilizing epidemic of a

highly virulent disease. In spite of this, protecting water reservoirs seems to attract much attention from mayors and governors around the country. They are proposing a $4-billion program to protect our water reservoirs, when such contamination presents a minimal to negligible risk.

We see little prospect of interdicting those who might carry bioterrorism weapons. They can move them, in very small quantities, across borders, with little difficulty.

Detection at the time of release had seemed to be a very attractive idea. Many companies have produced detection devices. None look promising as candidates for widespread use. A significant problem is the occurrences of false positive reactions. Even one such alarm in a large building in the course of a year could result in serious problems

We identified training of medical and public health personnel as a key need. We must depend on physicians, primarily those working in emergency rooms, to report cases they have never seen before and for which they do not have training. We are looking at a fairly simple set of measures. We need to detect the organism or the fact that the organism has been released. So we need to detect possible cases very early. This is where we begin. These physicians would then call on public health people to say they have got a problem that needs to be defined. But this must take place in a public health infrastructure, which is virtually nonexistent in many, many municipalities, and very weak at the state level. To investigate, we need laboratories to identify what the organisms are. But these organisms are not usually looked at by laboratories, so we began with virtually no capability to diagnose.

Another problem we identified is where to house a surge of patients. At the present time hospitals are running very near to capacity. They are financially strapped and short of personnel. Many of the hospitals in major metropolitan health settings could not accommodate a sudden surge of 50 acutely ill new patients.

There is no question that we are facing many problems here. What are we doing about them? On January 10, 2002, a budget for the Department of Health and Human Services was signed by the President that was directed toward public health preparedness. Initially, the problem, as we see it, is to try to do what we can as quickly as we can to counter an outbreak should it occur. The budget this year is

for $3 billion, which is six times what the Department received last year ($500 million). And the President is asking for $4.5 billion for next year. The Office of Public Health Preparedness has the responsibility to set the agenda. It is a formidable task. As one staff member said, we have tried to get attention from the public, Congress, and our colleagues for the last three years. We have been in the desert, praying for a little rain, and suddenly we are hit with a typhoon. It is indeed overwhelming.

We have determined our first steps. We must strengthen our public health infrastructure and we must build our communications network so we have communication between public health, emergency rooms, and infectious disease specialists so that cases can be quickly diagnoses and appropriate measures taken to control the outbreak.

We now have a network of 81 laboratories capable of diagnosing a number of these agents and regularly testing to maintain their proficiency. Smallpox is a priority. Although smallpox has a minimal likelihood of release, the catastrophe that could occur were it to be released worries us greatly. We contracted for over 200 million doses of vaccine, with the desire to have it by December 2002. We are a little ahead of schedule at the moment. We should have plenty of vaccine by autumn of this year.

Until now, the anthrax vaccine had been produced by a method perfected in the 1950s. It is now produced in a fully certified laboratory. We see the possibility of a recombinant anthrax vaccine being available and we have put that vaccine on an 18-month delivery schedule. Such a vaccine should produce adequate protection with not more than two doses.

We are also working with the states. Since January 2002, a billion dollars have been distributed to the states, with a provision that they can spend 20 percent of this and then come back with plans and timelines to get more. Those plans are coming in to us at the present time. We also have a tremendous amount of regional planning going on to accommodate at least 500 new acute patients in hospitals in each municipal area.

More laboratories are being built so we will have more competency. Communications networks are being developed to connect the public health system to hospitals and laboratories and to police and emer-

gency medical services. We are moving ahead at a considerable pace, but there is much to be done.

Problems Ahead

Bioterrorism is not going to go away. We have already had a release of anthrax of very high quality. That material was not produced by somebody who picked up a little something in his kitchen and produced weapons-grade anthrax. This effort required many chemical reactions and a lot of experimentation. It is safe to assume that whoever produced this anthrax can produce more. We do not know the source of production or whether it was foreign or domestic. The most important question is when the next release will occur, and that worries us very greatly.

We have got to be better prepared at domestic, civilian levels than we are right now. But that is not the only problem we are facing. We are also facing a new era in biology. The biology of the 21st century is going to be very different. We have many people now with capabilities in microbiology who can do all sorts of things in recombinant work. We have already seen some fascinating work, such as taking a gene from the Ebola virus and putting it in HIV. Many new combinations are being made with various organisms, and I think with all good intentions. But is it possible that one of these can escape from a laboratory? If so, what kind of controls should we have? And if you do put controls on, how much do we inhibit legitimate science? We are just beginning to discuss these issues. At this time, we do not have many good ideas as to how we are going to balance the needs of security with the needs of research.

We are also facing many new and emergent infections. We were startled when HIV appeared and now we have an epidemic. Will we have more epidemics? Yes, of course. But, now, populations are greater, and many people live close together in huge urban environments. In tropical areas, many people live in close quarters with virtually no sanitation. The potential for organisms to continually mutate and become established and then spread is certainly there, better than ever before in history. We will see more of these epidemics.

So we are facing not only the biological weapons, but also new and emerging infections, the potential for recombinants, and various new organisms being created. All of these issues must be on our agenda.

Conclusion

The President has asked for much more money for the research budget of the National Institutes of Health next year, some $1.5 billion in all. This money would give us the potential to do a great deal more than we have done. How we are going to determine what is needed in a practical sense and match that with the basic research agenda, looking ahead 10 years, is not very clear. We have a monumental task ahead.

4 One View of Protecting the National Information Infrastructure

Eugene H. Spafford

As we think about the threats to information technology, we may wonder what the real threat is to the public. After all, disruption of eBay, Amazon, Google or online chat groups does not seem like much of a menace. It is actually the amplification of other threats that is disturbing. Imagine if a few months from now we suddenly have an outbreak of a new variety of hemorrhagic fever. Cases begin to appear in emergency rooms at a dozen hospitals in a dozen cities around the country. Within two or three hours after the story hits the national news wires everyone becomes aware of the outbreak and we begin to marshal our resources. But the Internet goes down, along with 50 percent of the national phone network, and neither comes back up. Most people who boot up their computers get a message that says "Death to the great Satan," and then their disk is erased.

How many would be able to respond effectively without phones or network resources? What kind of panic would ensue? While thinking about this question, consider that our government has decided that cost is more important than quality. They use a monoculture computing system that has a compromised (and some would say,

---

Eugene H. Spafford is professor of computer science, professor of philosophy, and director of the Center for Education and Research in Information Assurance and Security at Purdue University. *This chapter is based on remarks delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy held April 11-12, 2002, in Washington, DC.*

minimal) immune system. It is being used for weapons guidance, national defense, government, and communications. Most people use the same system on their personal and business computers. Currently we are seeing new computer viruses and worms, targeted at that platform, reported approximately once every 75-90 minutes, on average. Extrapolating from the last 12 years of data, we may be seeing a new virus appear for this platform once every 30 minutes by sometime in 2003.

This system is the one on which we base our defenses, our economy, and much of our scientific enterprise. It is increasingly under attack from malicious software, in addition to a continuing litany of crashes, bugs and associated patches. And I have not even touched on the problem of hackers and automated attack tools, which may actually pose a larger threat than viruses as time goes by. The infrastrucure is built on shaky ground.

One recent study conducted in cooperation with the Federal Bureau of Investigation revealed that companies lose, on average, over $1 million each per year from computer misuses and computer crime. Worldwide, as much as $1 *trillion* may be lost in downtime and damages each year. Not only is poor security costing us real money, it is also harming our national competitiveness.

Looking at the current state of the practice in research makes the picture even more dismal. Nationally, we are producing, on average, about seven new Ph.D.s a year with in-depth knowledge of information security obtained at the leading educational institutions in this field. Based on recent trends, we can expect that two to four of them, on average, will return to their home countries each year, and perhaps three will take positions in academia.

Nationwide, we have no more than 100 (and perhaps as few as 60) faculty who have real training and expertise in this area and who are teaching in higher education. If a particular group of about 10 of them decide to retire or leave, we might lose two-thirds of our research centers in this area. Currently, the Federal government is investing no money in these centers to keep them running, so a lack of other resources might well have the same end result.

As best as I can tell, the total amount of money available this most recent fiscal year for *basic* research in information security was about $2 million (through the National Science Foundation); a great deal of

money is being spent on acquisition and development of technology for security, but that is money spent on extensions of known methods rather than basic research.

That is, in brief, the current state of information security in the United States.

Background

A little background may help us understand where some of the problems are and potentially where some of the solutions lie. Part of our current situation has to do with the speed at which information technology has progressed.

Forty years ago, we saw the creation of the first academic program in computer science as a discipline. This happened at Purdue University, with a few others created shortly thereafter. Thirty years ago, there were no large-scale networks. Everything was mainframes. Twenty years ago, the ARPANET had 231 nodes on the network (which was considered huge); today, although we have no way of getting an exact count, it is estimated there are as many as 300 million hosts connected to the Internet. Ten years ago, the World Wide Web protocol was developed. Commercial use of this network started only about seven and a half years ago. The World Wide Web now supports tens of billions of dollars worth of electronic transactions each year. The rapidity of the development of all this technology has certainly played a role here, as has some of the changing nature of the goals of the systems.

As we add more systems and as the growth continues, we also see a number of interesting emergent effects. This is not surprising given the increase in the complexity and size of the network. The amount of traffic that we see on the backbones of the networks has been doubling approximately every 90 to 120 days. That is an incredible increase in the amount of traffic. And the number of people estimated to be online has been doubling about every eight to 10 months for the last decade. Try to imagine any other kind of environment where you can continue that population growth reliably. It has strained our ability to cope with what is going on.

The Problems We Face

As I mentioned above, we have a significant shortage of professionals in computing science in general. At the undergraduate level we are producing only a fraction of the needed personnel, with some estimates indicating several available positions for each new graduate. Trend figures from the Computing Research Association's Taulbee Survey indicate that we have had a slight decline in the number of graduate degrees awarded in this field. At the Ph.D. level, nationally we are only producing enough Ph.D.s to stay even with the current number of computer science faculty in major universities—and there are certainly not enough graduates to satisfy the need to grow departments. In addition, currently, 57 percent of the graduate students in computer science in this country are not U.S. nationals. Only about 12 percent of our students are female. Other underrepresented minorities are an even smaller percentage, unfortunately.

Information security is an even smaller component of this population. Why? In large part, because there is huge market demand. It draws away people well before they go on to advanced study or teaching. It is a very small community to begin with and the market demand shrinks it even more. The demand is so great that many companies are hiring former criminals and confessed vandals as security experts. This is incredibly poor business sense (would you want a "reformed" arsonist to install your fire alarms?), but poor technical sense as well: most systems are so fragile that kids can become experienced system hackers without any real technical depth.

This incredible demand not only pulls people out of academia before they complete their training in information assurance, but it also has led to companies hiring individuals without sufficient training in basic computing. Many of the major software firms have been so desperate to get anyone who knew how to write a program that they have hired people who have only a high school diploma. In fact, they have hired some people before they finished high school whose entire education in software engineering may have been picked up in an introductory book. The code they write, their engineering and their designs form the foundation for our national (and global) information infrastructure. And there is a woefully small cadre of information assurance specialists to help shore it up. It is a grim picture.

High market demand is only one of the issues we must deal with. The speed of the market is another. In producing software, time to market is a critical business decision and simply one factor in the speed of the market. If you take six extra months to design and test your software carefully, you may be preceded to market by another firm in the same area and you would lose your opportunity to dominate. Getting there first is now more important than getting there correctly.

One result is that companies no longer do so much as beta test their software. Instead, they market it with disclaimers, anticipating that they can patch it in the next release. This is complicated by the fact that the Internet is a marvelous distribution channel, which can be used to disseminate software with no shipping cost and very little advertising. You simply put something up on a Web site; then people find and download it. That is also a very convenient mechanism for patch distribution—one can ship the next emergency patch over the Internet with almost no additional cost. It also means that because patches and configuration options are so available, there are no standard configurations to test to anymore.

There is no standard version of software anymore, partly because of the speed of the market. Demand trumps issues of quality and safety. We have all kinds of eager adopters who are enamored of the technology and who want the latest, greatest, and newest features. They are willing to download marginal software, install it, and run it in a risky manner simply to have it.

Technology trumps management in this regard. Trying to set policy to prevent people from downloading early-release versions and forcing them to run a standard configuration runs the risk of rebellion. Preventing employees from browsing Web sites during office hours is enough to cause them to leave companies and go to work elsewhere. If the employees are computer savvy, they can easily find new positions, so management is reluctant to enforce basic controls. This means we have real problems in security management.

One approach is to impose technology that works as a network nanny, as it were, to guard what people are browsing at work, or to set up firewalls to prevent users from downloading risky software. The problem with this technology is that you are trying to prevent technology-literate individuals from doing something that they want

to do. They can—and will—find ways around it.

Another problem involves the vendors. They are annoyed that management is trying to keep out their advertisements. As a result, they create protocols and methods to circumvent security.

Another issue is that of liability. Vendors produce goods they know are bad. Not only is there no feedback, there is no liability. The vendors are spending a considerable amount of money trying to get legislation passed to shield them from lawsuits. The Uniform Computer Information Transactions Act, a modification of the Uniform Commercial Code, is being lobbied very heavily by a number of manufacturers for passage at the state level. Virginia and Maryland have already passed it. This law allows the vendors to disclaim all liability and to actually prohibit individuals from writing anything critical about their software for publication. It is rather frightening how that is being pushed.

Cost is pushing organizations, including government, to adopt unsafe technology because it is inexpensive. This is akin to the U.S. Air Force buying cropdusters because they are cheaper than F-16s or the U.S. Navy buying bass boats with outboard motors because they are inexpensive. But that is effectively what we are doing with software. The next generation of Navy aircraft carriers is going to have all weapons systems, propulsion, and command and control run by the very same system that you use at home to browse the Internet and play computer games. This is the same one that keeps coming up with "blue screens of death," which take on new, grim meaning in a military environment. This is a problem, in part, because those systems are made to sell to everybody. They have the lowest common denominator features and the simplest policy. Demand, again, is part of this. Vendors have to sell to people who have no computer training, many of whom are actually functionally illiterate and could not understand the manual if they wanted to.

If companies put in security controls and turn them on, the volume of calls for help increases many fold. Right now the margin of profit is so slim on much of the software that doubling the number of calls for support would make the product lose money. To remain profitable, they turn off all the confusing features—including all of the security features—that might limit the interoperability of the systems.

We also have a preference for fads, which is part of the issue of

demand over quality. The excitement over wireless computing is an example. Little or no thought is given to the dangers behind that—how easy it is to disrupt, how easy it is to eavesdrop, and all of the various implications behind the lack of security in wireless networking. Another technology in vogue is browsing the Web on cell phones. The convergence that is going on here is dangerous. Although not always reliable in an emergency, cell phones could at least be depended on for stable software. Now companies are marketing, because of user demand, cell phones that allow you to download new features and actually run programs on them. Thus, we are now seeing viruses for cell phones. So you cannot depend on that platform anymore. We are introducing new means of instability because of user demand.

From a policy standpoint, we are seeing, both in industry and in government, incredible investment in short-term solutions but almost none in long-term ones. We need to do basic research in issues of security, not only to develop better approaches, but also to build the next generation of researchers. Instead, most of the research investment is being spent on developing new methods of downloading patches for the same old buggy software, new methods of putting up firewalls to protect the same old buggy software, and new methods of virus protection for the same old buggy software. That is not going to advance us very far toward the next generation of technology.

We have a number of policy decisions that are being made by low-level technical people. They are designing protocols and systems to do what they think is interesting and to push the edge of possibility. Their work is finding its way into the marketplace and it is being adopted. We end up with protocols that are built simply to work, without any concern for issues of resiliency and accountability. For instance, right now, being able to determine where anything comes from on the network is next to impossible. As a result, we are seeing all kinds of emergent problems that were not anticipated and that we have very little ability to deal with. Spamming is one example. A recent study done in Great Britain revealed that 40 percent of the traffic that goes through their commercial Internet service providers is now spam. The Gartner Group has said that spam is basically doubling every four to six months. Spam alone may take down large portions of our network!

We do not have a lot of training going on in the area of regulation and law enforcement. In the last 20 years, almost everybody I have met from law enforcement who has learned enough about computing to do forensic analysis has been able to go into industry, working in software engineering or production, at two or three times the salary (and they do not get shot at as often). Few stay in law enforcement very long. Thus, we do not have the technology there, and the law is certainly not helping us. The criminal law lags behind, as it probably should, but it makes it difficult to do some investigations and enforcement.

We also have the major technology firms pushing for special interest legislation that actually hinders research. Many of the large intellectual content providers, such as Sony and Disney, have supported laws such as the Digital Millennium Copyright Act. This law makes it actionable for a researcher to perform many kinds of investigation into the weaknesses in copy protection protocols. If I were to do work in forensic technologies, I technically could be sued by any of these companies or arrested simply because I am investigating ways to break through security on malicious software—but which could coincidentally be used to circumvent their copy protection methods. Thus, if a company needed to reverse engineer a computer virus to derive a countermeasure, they would be violating Federal law—as would the vendors of any tools to support this effort. If the DMCA had been passed before 1999, most of the technology and efforts used to remediate Y2K problems would have been illegal!

Another bill has been introduced in Congress that would require hardware and software technology to prevent copying without approval from one of these companies (the Consumer Broadband and Digital Television Promotion Act: CBDTPA). It is being discussed as something to save the entertainment industry and promote the use of broadband, but, actually, it will severely weaken information security and reduce our ability to do research and communication.

So these are some of the factors–the high market demand, the push from industry, the interest in short-term results, and the primacy of cost over quality—that make this such a difficult domain. Few individuals work in the area of information assurance and there is little support for what we are doing. Our work is viewed as damaging to

those commercial interests or as increasing the cost of technology. So we are not supported so as to make a lot of progress or respond to some of the problems that are out there.

Steps to Solving the Problems

How can we make a difference? We can be better consumers. We can buy tools that have better quality and are better suited for what we need to do. For example, earlier I mentioned how the Microsoft family of software has tens of thousands of known viruses, and new ones are being reported at a rate of dozens per week. Macintosh OS 9 has fewer than 60 viruses in total, almost none of which run under native OS X (notwithstanding the viruses for Microsoft Word). Unix and Linux have about three. I leave it up to you to decide if this is the sort of factor that should make a difference in what someone should deploy in a security-critical environment.

Second, government and industry need to invest more resources in information assurance research and education. Otherwise, we are not going to see much progress towards the long-term solutions: we are going to be continually in the cycle of patching old problems.

Third, we need to see a significant, prolonged investment by government and industry in building up our research infrastructure, educational resources, and personnel base in information assurance. This requires funding both individual researchers and centers, and including sufficient resources to enable significant basic research.

Fourth, we have to start doing something to hold the vendors and the perpetrators of this mess responsible. Vendors know how to put in better quality. I could write another chapter on how 30 or 40 years worth of research has generated basic principles that are being ignored because they add to the time and costs involved with production. The same kinds of arguments that are being used now by the software firms are the ones that were used by some of the tobacco companies. We should not tolerate that.

And lastly, we need to understand that security is not an add-on. It has to be designed in, and pursued as an on-going goal of operation. There is very little we can do with existing systems now to add something on that will address the majority of risks. All we can do is increase the difficulty of someone exploiting obvious problems. But

security has to be built in as a fundamental, and that simply is not the culture. That is not the tradition and we do not have the infrastructure in place to fix that.

In conclusion, it is hard not to be somewhat pessimistic when being realistic, after looking at what has been happening over the last decade or so. If the consumers, vendors and government would all make quality and security a priority, we might begin to see a change; I'm afraid it may require a major disaster before that happens.

Acknowledgments

Thanks to Mike Atallah, Becky Bace, Matt Bishop, Steve Chapin, Simson Garfinkel, Steve Hare, Jim Hendler, Pascal Meunier, Ken Olthoff, John Richardson, Marv Schaefer, and Gene Schultz for comments on an earlier draft of this document. The opinions and interpretations expressed in this document are mine alone, and do not necessarily reflect the opinions of any of these individuals.

5 Assessing and Communicating the Risks of Terrorism

Baruch Fischhoff

Assessing and communicating the risks of terrorism requires the collaboration of the full spectrum of social and behavioral sciences. This chapter discusses research that we could and, were we to be responsible, should apply to the problem of terrorism. I will also give a feeling for how we might do the kind of systems engineering that Dr. Lewis Branscomb calls for in Chapter 2 of this volume. This will require integrating the social, behavioral, natural, and engineering sciences.

This chapter examines, in turn, the psychology of risk (both for experts and the public); risk analysis and risk communication (and how the two must be integrated for either to be effective); special considerations in the domain of terrorism; how we might begin to apply these perspectives to bioterrorism; and, finally, some areas where we might immediately begin to develop applications and conduct the supporting basic science.

The Psychology of Risk—The Public

The public is important in our response to terror, both as actors and as audiences. We need to communicate with people well in advance of any terror-related crisis. They need to have some idea of

---

Baruch Fischhoff is university professor in the Department of Social and Decision Sciences and the Department of Engineering and Public Policy at Carnegie Mellon University. *This chapter is based on remarks delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy held April 11-12, 2002, in Washington, DC.*

what is going on, in order to have a chance to make effective decisions, being as heroic as they choose—without feeling they were misled or incompletely informed.

Understanding the psychology of the public is also important for anticipating how people will respond to our plans. For example, Dr. Eugene Spafford's paper (Chapter 4 in this volume) discussed various plans for protecting our computer systems. Each plan assumes some behavior by the computers' human operators, such as respecting one another's privacy and protecting one's own. If we do not understand human behavior, then we have *behaviorally unrealistic* plans. Including the human sciences adds a level of complexity to already complicated planning processes. Yet without them, we are blinding, and perhaps deluding, ourselves.

One long-standing focus of research into the psychology of decision making is how people's current beliefs shape their future understanding. Knowing the details of these processes is essential for effective communication. If we do not know where people are coming from, it is very difficult for us to get them to another place. People's ability to process risk communications depends on their numeracy and literacy. Numeracy is required to understand how big risks are (and how much risk-reduction measures will cost). Language literacy is required to process written messages. Scientific literacy is needed to grasp the content of messages that, with terror, can involve a large number of domains. For example, we need to know something about anthrax, about the (foreign or domestic) people who may be behind an outbreak, about diffusion rates for small particles, about the management responsibility of various government agencies, and so on. How well one can understand the anthrax crisis depends on one's literacy in these different domains.

People's responses are also constrained by their limited cognitive capacity, which can shrink further under crisis conditions. Given these limits, people manage to function either by acquiring domain-specific knowledge or by relying on robust, but imperfect *heuristics*. These "rules of thumb" simplify problems and provide approximate answers. But they can also produce biases. For example, people seem to count, almost automatically, how frequently they see various events. Those estimates can be useful in estimating the frequency of such events—unless appearances are deceiving, such that some

events are disproportionately visible, leading to overestimating their actual frequency. People may not often think about the representativeness of the evidence that they see. When they do ask that question, they may not adjust adequately from what they have seen to what is actually there.

Researchers relying on psychological theories and methods have found it possible to increase people's understanding of many risks. Nonetheless, some concepts are inherently difficult to communicate. One challenge is giving a feeling for very low probabilities. We have 285 million people in the denominator, when thinking about the risk of terror for an individual in the United States. However, our perception of these risks may be unduly influenced by a relatively small number of very salient incidents in the numerator. A second challenge is conveying notions of cumulative risk, arising from repeated exposure. A particular event might be very unlikely on a given day (or trip), but over time, those tiny probabilities can mount up—and at a rate that people do not realize. A third problem arises with verbal quantifiers like "likely," which can be very confusing. "Likely" means different things to different people, and different things to the same people in different situations. If you try to communicate the size of risks using words instead of numbers, you are setting a trap for your audience.

People have difficulty making decisions about events that they have never experienced. It is hard to project oneself into unfamiliar situations. As a result, we have difficulty predicting our own responses to events. A growing literature shows how decision-making difficulty can reflect uncertainty about ourselves (or "value uncertainty") as well as uncertainty about the world. In effect, we do not really know what we want in many novel situations. Difficult medical decisions often evoke such feelings.

Our responses to risks reflect our emotions, as well as our beliefs. Emotions can both confound and support our cognition. They can empower us to act, but also paralyze us. They both affect and reflect our beliefs. Terrorism evokes a wide range of emotions, which must be understood if we are to aid and predict citizens' choices. These emotions include fear of the effects of terrorism, frustration with ourselves and our authorities, mourning, and solidarity with our fellow citizens.

The Psychology of Risk—The Experts

Experts have uncertain beliefs and emotions, too. Novel situations may draw experts into areas that no one understands very well. They may need to interface with other experts, from unfamiliar disciplines. As citizens, we need to understand the psychological processes of our experts, in order to decide how much we can trust them. As experts, we need to have—and to convey—a realistic assessment of our own competence, if we are to merit the public's trust. We need to define our domain of expertise and be willing to coordinate with experts from other domains.

We also need to have a clear, consistent public role. We can try to inform people or to persuade them. That is, we can provide facts or we can provide spin. But we cannot mix these roles. If we do, we will confuse our audience, who will not know how to interpret our claims.

Because the problems of terror are so new, they force new groups of experts to communicate with the public and, in doing so, to demonstrate their competence and honesty. There is, however, a learning curve for talking to people about risk. Experts must make rapid progress on this curve if they are to earn trust that is hard to restore, once lost. Unfortunately, a natural first response for many experts is telling citizens to "go away while we do our work." If people persist in wanting to hear about the risk, it is tempting to tell them what they ought to think—rather than leveling with them, and providing the facts that they need for independent choices.

It is tempting, sometimes, to magnify risks in order to motivate citizens. At other times, it is tempting to trivialize their worries, with comparisons like "why get so exercised about terror, when you're still smoking" or "only five people have died from anthrax [so far], compared with 40,000 annually from motor vehicle accidents." Except for extreme situations (e.g., rapid evacuations), experts must seek a partnership with the public.

We saw the result of confused expert roles in the anthrax crisis. We also saw experts disparaging the public, reflecting the limits to their own psychology. Experts may be biased by their limited opportunities to observe the public—and their failure to recognize the un-

representativeness of what they see (i.e., how citizens appear in heated controversies, "person in the street" interviews, or responses to ambiguous survey questions). Experts may also have ego involvement in how the public is viewed. They may show professional arrogance and defensiveness. They may be concerned with defending their own expert status, hence benefit from deprecating the public. They are just people, also feeling the pressures of the times, whatever their professional training.

Risk Analysis and Communication

One way of disciplining expert judgment is to perform formal risk analyses. That means identifying valued outcomes, the processes affecting them, and the experts with the best understanding of each. These experts must be asked to pool their beliefs, uncertainties, controversies, and omissions—then subject their work to independent peer review. In principle, risk analysis is no different than any other modeling process. Yet, in any new area, analytical conventions need to evolve. Without them, relying on experts' intuitive judgments may create misleading pictures.

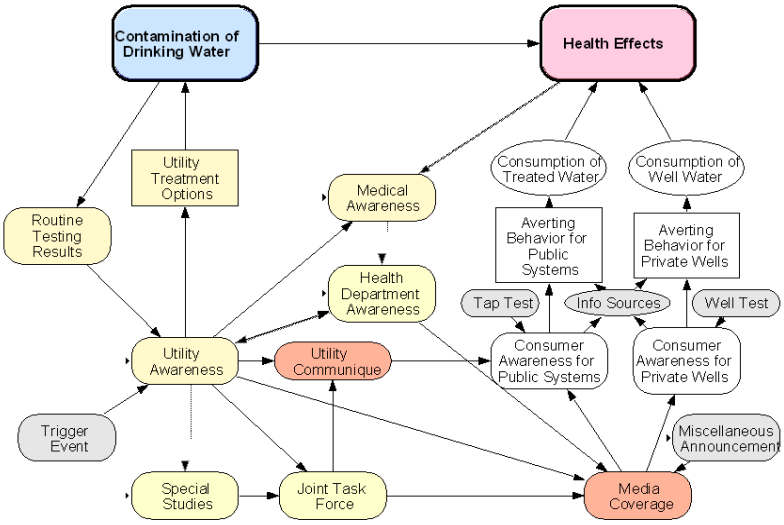
For example, we recently conducted a risk analysis for contamination of domestic water supplies by *cryptosporidium*, a water-borne parasite. Milwaukee had an outbreak about 10 years ago, where about 100 people died and 400,000 got sick. We were asked to develop the perfect "boil water" notice. Through interviews, we found that many people did not know how to boil water effectively. We also found that many people would want to know who produced a notice, before deciding how seriously to take it. Thus, a boil-water notice might need to explain the risk management system that produced it, in addition to instructions about what to do.

Figure 1 shows the top level of our risk analysis model (led by Liz Casman, a microbiologist.) It integrates the engineering science of managing water supplies, the biological science of parasites' effects on our bodies, the communication science of how messages get organized and disseminated, and, finally, the psychology of what happens when people make such risky decisions.

Once we completed the model, we asked what contribution a perfect "boil water" notice would make, assuming that everyone re-

ceived and believed the notice, then boiled water the right way. How would this affect a typical epidemic? We ran the numbers and found that it had no effect whatsoever. It took us a couple of anxious weeks to understand what was happening. We hoped our sponsor would not call during this period. We finally realized that with current detection systems, *cryptosporidium* would have already done its damage before anyone knew that it was there.

Figure 1
A Risk Management System for *Cryptosporidium*



Thus, the tests are good for forensic value, determining what hit you after an epidemic, but not for protecting public health. We had a public health system built on unrealistic psychological and engineering assumptions. However, we did not realize this until we actually did the analytical work. Having done so, we realized that the system had misplaced its priorities. In this case, we should not be putting money into better communication, but into better testing technology or into land-use practices that reduce intrusions. Believing in the cur-

rent system means not routinely providing immunocompromised people with bottled water, needlessly exposing them because we had not analyzed the system.

At this time, I was reading some brochures published by the National Cancer Institute (NCI) on how to deal with chemotherapy. They were very nice brochures, but said nothing about risk from water-borne sources. I called some colleagues at NCI and at the Centers for Disease Control and Prevention. They said that they had thought about this risk, but somehow that concern had never found its way into the system. I talked to the person responsible for the brochures who said, "That's a good point, but we just printed several million of them. Call us back when the supply runs out." This example shows that we have to set priorities explicitly. If we are not systematic about this, we may invest our money in the wrong places and expose people to needless risk.

Once we have figured out which facts are important to know, developing risk communications is relatively straightforward. First, we need to determine what information is common knowledge, hence goes without saying. Knowing what people already know avoids wasting their time and losing their respect (by not giving them credit for that knowledge). Such common knowledge can be identified with open-ended interviews, allowing the full expression of intuitive beliefs, values, and formulations. Structured surveys allow estimating the frequency of different beliefs.

The next step in designing communications is characterizing the critical gaps in lay beliefs, representing what is worth knowing. Many risk situations require understanding both quantitative information (how big a risk is, how much it will cost to reduce it) and qualitative information (what determines the risk, where it comes from, how it is assessed, how it reveals itself in everyday life). One then needs a story line to communicate the information that matters. People need a coherent mental model, giving qualitative meaning to the quantitative statistics, building on the constructive processes of learning and memory. The success of any communication must be empirically evaluated. We have been studying these topics for 25-plus years and still are surprised by what we learn from the testing process.

The Special Challenges of Terrorism

What is special about terrorism within this general context of risk analysis and risk communication? One important feature is the diversity of people who must work together in order to address these very complicated problems. They need to create broadly shared mental models in order to coordinate their actions and beliefs. They also need to reconcile their mixed motives. In addition to fighting terror, their actions will affect their own status and our society. For example, airport security is about flying safety, but also about the respective roles of the public and private sectors in our society. As citizens, we, too, have mixed motives. We want facts, but also reassurance. We want to know whom to blame, but also to feel solidarity with our fellow citizens.

A second feature of terror-related events is that they challenge the validity of our experience. This is novel ground, even for the professional community. We must deal with unfamiliar topics, unfamiliar people and places, and unfamiliar pathogens. As a result, terrorism requires theoretical understanding to augment the historical statistics. Because the old statistics may not be valid for the estimating, say, aviation or anthrax risks, we need models integrating these theories. Unless we recognize and interpret these pieces, we are working at cross-purposes.

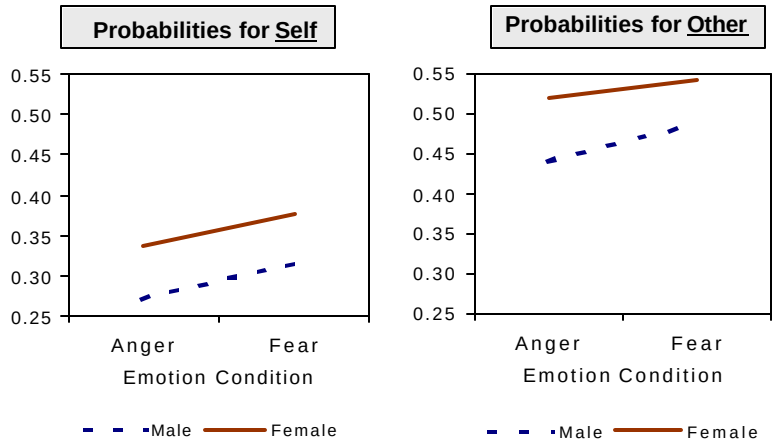
A third distinguishing feature of terror-related events is the intensity of the emotions involved.

We were able to conduct a study examining the effects of these emotions on risk judgments (with support from the National Science Foundation). We had access to a random sample of a thousand Americans, through WebTVs in their homes. We experimentally heightened three emotions that are naturally associated with terrorism—fear, anger, and sadness. For example, the anger group saw a picture of people supporting Osama bin Laden, with a voice-over of quotes from CNN and *The New York Times*. They also wrote about their anger regarding the events of September 11. A second group received a fear prime (showing gloved postal clerks sorting mail), while a third group received a sadness prime (a woman reading a letter from her husband who had died at the World Trade Center).

A precursor to our study was recent research showing that angry people tend to be more optimistic, and see lower probabilities of bad things happening to them. Before this finding, researchers generally believed that all bad emotions went together: People who are depressed also feel hopeless, and so on. But anger is a different kind of negative emotion.

Figure 2 shows these individuals mean judgments of the probabilities of eight risky events, summarized so that higher mean probabilities indicate higher perceived risk. The figure shows that people made angry about the attacks were more optimistic about their prospects.

Emotion & Gender Effects on Terror Risk Judgments
(mid-November 2001; n=973)



The figure also shows that women see greater risks than men. This result is consistent with other research finding that women report lower degrees of anger than men—as was found here as well, both for the anger that they brought with them to the study and their responses to the emotion primes.

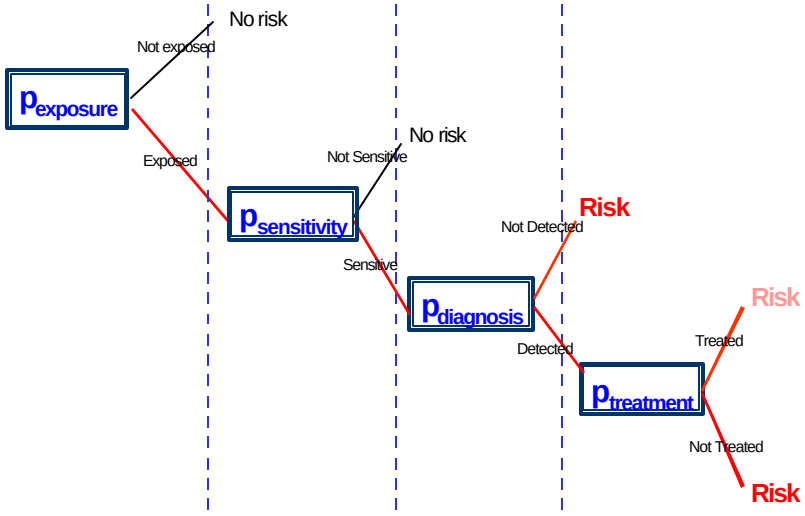
Many previous studies have found that people believe that others are at greater risk than they are. The comparison between the two graphs shows a replication of this result. The graph on the right shows the mean risk for the "average American." The graph on the

left shows the average of these average Americans' judgments of their personal risks.

A Worked Example: Bioterrorism

Last fall, I was on a panel with Dave Piposar from the Allegheny County Department of Health. He described how his department was dealing with the flood of anthrax-related calls. He said that one thing that people did not realize is that they have to be exposed in order to have a risk. In thinking about how to organize a risk analysis that would serve the communication needs of these callers, we produced the very simple model of Figure 3.

Figure 3
A Common Structure for Bioterrorism Risk

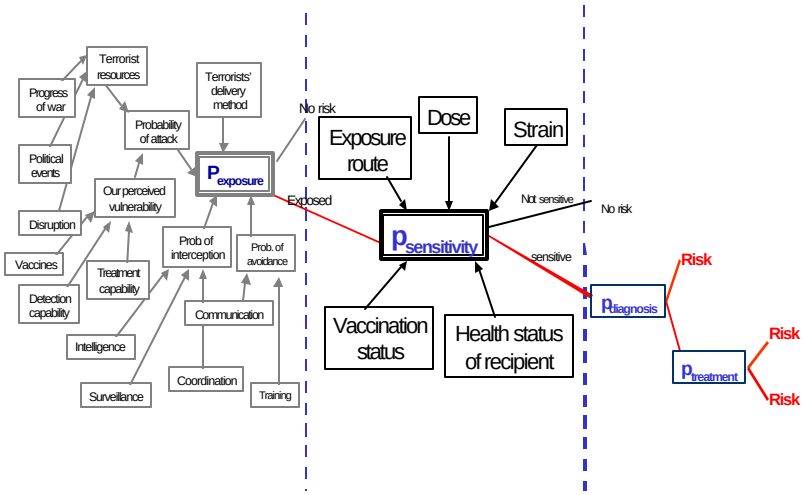


In order to have a risk from bioterrorism, you need to be exposed and you need to be sensitive at that dose. You need to miss the diagnosis or get the diagnosis right and have treatment fail. Thus, these risks have a multiplicative structure: everything needs to go

wrong. An effective communication would recall the full picture, even if focused on a specific issue in it.

Figure 4 shows a set of things that one would like to know in order to predict the probability of exposure. Conducting such analyses requires a team with expertise in each node. If we have not assembled that team, then we are not doing our job. Missing issues entirely may be more problematic than inaccurately measuring an issue that is considered.

Figure 4
What Determines the Probability of Exposure?



Producing such an integrated model is important, even if we do not "run the numbers" to produce quantitative estimates. It forces rigor in specifying variables and relationships, and in identifying relevant expertise. Given such a model, one could rapidly update it, if the situation changed. One could use it as a basis for estimating the risks of an outbreak of smallpox. Smallpox is different than anthrax because it is contagious. But many of the processes in the anthrax model recur with smallpox and many other disease agents, even when the details are different. The science that went into building the first

model could be used again in others. One could also look for processes that recur in multiple models, such as the enemy's probability of attack, our response capability (monitoring, coordination, etc.), and other valued consequences. We should invest in studying those crosscutting issues.

Like other risk analyses, such a model provides a guide for risk communications. It shows how to structure the long-term education needed to give citizens the big picture represented by the model as a whole, prepare them for the varying faces of the long struggle to come. It shows how to get ahead of the game, preparing and evaluating communications for crisis use. To the extent possible, such real-time risk communications should have a common (and pre-tested) structure for topics like exposure and detection, and a common format for expressing risk levels and uncertainties. Everything should reflect the science of risk communication.

Another topic requiring advance research is dealing with false alarms. We need to maintain consistent alarm standards (as proposed by Governor Ridge's color-coded alert levels). Explaining the philosophy underlying them will help citizens to understand why false alarms are inevitable and minimize their costs—including cumulative apathy. When false alarms do occur, we need to minimize both disruption and the perception of cover-ups.

A third research topic is how to deal with the second-guessing that follows terror-related events, neither succumbing to hindsight bias nor hiding behind it. Learning from the experience requires considering our leaders' entire decision-making process. Could they have acted on their knowledge? Was leadership possible? What did they know? What could they reasonably have known? How clear was the signal? We must judge the quality of their choice, not its outcome. These inquiries, too, should be guided by the science of decision making.

As mentioned, the public may be second-guessed by experts who doubt citizens' competence. Here, we must distinguish between ignorance and stupidity. How good was the communication to citizens? How defensible are their misunderstandings? How good is our evidence about the public? Evaluating citizens' actions requires knowing what problems they are solving. This includes understanding their options, values, and beliefs.

A fourth topic for advance research is setting priorities, linking public opinion with public policy. We need to present citizens with a full range of options and predicted outcomes, if we hope to know how they want us to respond to terror. We need a structured public discussion for how to pursue the long task ahead of us.

Our national survey asked about the relative importance of four priorities. We found strong support for two. One is that Americans want honest and accurate information about terror-related situations, even if that information worries them. This was true whether people were in the anger or the fear condition of our experiment. Second, we found very strong support for investing in general capabilities (like stronger public health) rather than in specific solutions (like smallpox vaccination). This policy was supported slightly less by people in the anger condition. Two priorities given somewhat less importance, were deporting foreigners who lack visas from the United States, and strengthening ties with Muslim countries.

Conclusion

Effective risk analysis and communication require quantitative estimates of risk (including the attendant uncertainties) and explicit representation of the processes shaping those risks. Producing them requires suitably diverse expertise. It also requires integrating risk analysis and communication, so we can solve people's problems and secure their trust.

Acknowledgements

I would like to thank Liz Casman, Matt Dombroski, Sara Eggers, Dalia Patina Echerverri, Paul Fischbeck, Roxana Gonzalez, Umit Guvenc, Jennifer Lerner, Deborah Small, Conrad Steenkamp, and the National Science Foundation, for their roles in the work reported here. The views expressed are my own.

Additional Resources

Casman, E., Fischhoff, B., Palmgren, C., Small, M., & Wu, F. (2000). Integrated risk model of a drinking waterborne *Cryptosporidiosis* outbreak. *Risk Analysis*, *20*, 493-509.

Fischhoff, B. (1992). Giving advice: Decision theory perspectives on sexual assault. *American Psychologist*, *47*, 577-588.

Fischhoff, B. (1995). Risk perception and communication unplugged: Twenty years of process. *Risk Analysis*, *15*, 137-145.

Fischhoff, B. (1998). Communicate unto others... *Reliability Engineering and System Safety*, *59*, 63-72.

Fischhoff, B. (1999). What do patients want? Help in making effective choices. *Effective Clinical Practice*, *2*(3), 198-200.

Fischhoff, B. (2000). Scientific management of science? *Policy Sciences*, *33*, 73-87.

Fischhoff, B., Bostrom, A., & Quadrel, M.J. (2002). Risk perception and communication. In R. Detels, J. McEwen, R. Beaglehole & H. Tanaka (Eds.), *Oxford Textbook of Public Health* London: Oxford University Press

Henrion, M. & Fischhoff, B. (1986). Assessing uncertainty in physical constants. *American Journal of Physics*, *54*, 791-798.

Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality & Social Psychology*, *81*(1), 146-159.

Morgan, M.G., Fischhoff, B., Bostrom, A., & Atman, C. (2001). *Risk communication: The Mental Models Approach*. New York: Cambridge University Press.

National Research Council. (1996), *Understanding Risk*. Washington, DC: Author.

Organisation for Economic Co-operation and Development. (2002). *Guidance Document on Risk Communication for Chemical Risk Management*. Draft, 6 March.

Performance and Innovation Unit. (2002). *Risk and Uncertainty*. London: Parliament.

Slovic, P. (Ed.). (2001). *The Perception of Risk*. London: Earthscan.

6 Research Universities and National Security: Can Traditional Values Survive?

Eugene B. Skolnikoff

This chapter discusses the specific impact the events of September 11, 2001 have had on research universities and of stresses and conflicts that have been raised. A real clash is possible over whether the responses that seem to be required by the threats of terrorism will conflict directly with the values that the universities feel are important to them and to their contributions in the fight against terrorism. The danger of overreacting is quite real, and in fact, I believe is already happening.

These "traditional values" actually go back only 30 years or so. But they are the values the research universities have come to accept as essential for high-quality education and research. The threats to these values are not new. We have seen many in the last few years. They include concerns about the impact of financial rewards on faculty, ethical issues posed by research, whether information is freely exchanged when important financial rewards are to be achieved, and the role of earmarks and of universities lobbying for them. But in this chapter I am focusing only on security-related threats to values. They predate September 11, but they are obviously much more pressing now.

Eugene B. Skolnikoff is professor of political science emeritus at the Massachusetts Institute of Technology. *This chapter is based on remarks delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy held April 11-12, 2002, in Washington, DC.*

The Values

I am concerned about four principal values: commitment to openness, resistance to classified research, maintaining open relationships between universities and industry (including foreign industry) and, of course, relations with foreign students.

The issue that has caused the greatest problem in recent years involves the commitment to openness and the free exchange of information that the universities believe to be central to their research quality and productivity. The issue grows out of the threat of proliferation of weapons technology to rogue states, that is, states that might challenge our military dominance and counter it in destructive ways. The primary venue has been the International Traffic in Arms Regulations (ITAR), a set of rules that control the export of items that are on the munitions list. The U.S. Department of State administers ITAR and implements the licensing process. If a project falls under ITAR, a license is required before any information can be shared with foreign nationals, including students and scientists.

The field most affected by ITAR so far has been the space sciences because of their close tie to ballistic missile technology. (But the language of the ITAR would allow it to be extended over any area of science and technology.) A major change affecting the space sciences occurred a couple of years ago when communications satellites were moved from the export control of the U.S. Department of Commerce (concerned with trade issues) to the U.S. Department of State (concerned with munitions control).

This move was a product of two egregious incidents in which American satellite companies were helping the Chinese to explain why they had two failures. In the process, the companies were accused of passing on information that was covered by the munitions list, without a license. One of the companies involved has just recently settled the case and paid a very substantial fine, mainly to get it off their books because of its effect on the rest of their business.

Fundamental research is specifically excluded from coverage of ITAR. Fundamental research is defined as basic or applied research, the results of which will be published without any restriction. There is considerable ambiguity about what fits that definition. For example, is it no longer fundamental research if a sponsor puts a brief hold

on publication or pre-publication in order to review the research for possible patentability? As I understand it, the State Department essentially says that any restriction of any kind on publication removes it from the fundamental research exclusion. For this and other reasons, it is often hard to tell in advance whether something is covered or not.

Even for fundamental research, another provision called "defense services" can negate the research exclusion. That is defined as providing assistance to foreign persons in the use of defense articles (i.e. anything on the munitions list). That includes "design, development, engineering, manufacture, operation, demilitarization, destruction, processing, or use of defense articles."[1] In other words, everything.

ITAR is comprehensive, complex, time-consuming, and often inconsistent. It often requires legal interpretation. Note that none of this has to do with whether information is classified or not. Unclassified information is also covered. Furthermore, it is important to note that anyone accused or convicted of violating ITAR is subject not just to fines, but to imprisonment.

So the issues become very personal and individuals in these fields are often quite aware of that. This has caused considerable unrest in the space sciences. Proposed contracts have been delayed and questions about foreign graduate student participation have been raised. Potential foreign collaborators have said they prefer not to work with Americans. Discussions at scientific meetings have been constrained or aborted. At times, meetings held in the United States have had to stop while foreign nationals were asked to leave the room and return later. Projects involving universities and industry collaboration have been delayed or canceled. Universities with limited staffs often simply do not have the capability to deal with these issues. ITAR has at times contributed to a climate of fear that has led faculty to withdraw rather than continue with proposed projects.

I recount the history of this subject because it shows what has happened in the past, before we became concerned with September 11 and its aftermath. The situation is just slightly better now than it was a few weeks ago. The universities, in general, and the Association of American Universities in particular, have made strong representations to the Administration about the problems caused by the ITAR, and the Administration has responded. After more than two years of in-

ternal negotiation, some amendments to ITAR have been added which have calmed the situation somewhat.

A major change is that public domain information can now be shared with foreign nationals from the North Atlantic Treaty Organization (NATO) and a few NATO-aligned countries without requiring a license. That is a substantial step forward. It greatly eases relations with our largest space collaborator, the European Space Agency, and with some other countries, particularly Japan. But some significant problems remain. Often, a seemingly sensible modification does not quite turn out as expected. For example, one of the amendments specifies that any information can be shared with universities or government research laboratories in NATO countries. That is fine, but it does not specify whether the partners have to pledge not to pass the information on to others from "unallowed" countries. That is left open.

Similarly, another amendment says you can deal with foreign students on these issues if they come from NATO or allied countries. But, in our universities today, we have many other nationalities represented. Does that mean that universities are asked to exclude certain foreign students from some projects and allow them in others? I believe that is absolutely unacceptable, but that is the direction in which we are moving.

Perhaps the most important part of the change brought on by these amendments was that the preamble restated a Presidential directive from the Reagan years (NSDD 189) that explicitly stated that fundamental research is in the national interest and all such information should be freely and openly disseminated. Information that has military or other security rationales should simply be classified.

As I noted above, the space sciences have been the focus so far, but the munitions list refers to any subjects that have military application and specifically mentions biological and chemical agents. I fear that it is only a matter of time before ITAR will be extended to those as well. My perception is that the climate in the government on these issues is such that, outside the science agencies, the concerns of universities are not well respected. There is considerable receptivity at the White House and perhaps at the level of agency leadership for these concerns, but not at the working levels of the government, particularly in the Defense and State Departments. Their responsibility

is a very different one. They may understand why the universities are dismayed, but the State Department's responsibility is non-proliferation and the Defense Department's is military systems. They do not accord much importance to the costs to the universities that may be involved nor much credence to the longer-range costs to national security that will result.

What Has Not Changed For the Research Universities?

One major continuing factor is the national nature of the scientific and technological enterprise. The majority of decisions about science and technology (S&T) are still made in a national context in which policies affecting S&T are determined in a domestic political and budgetary process. The research universities are, and will continue to be, dependent on the government. Moreover, the government has many ways to influence S&T, even though the private sector today gives much more funding support to research and development (R&D) than in the past. Regulations, subsidies, patent policy, trade agreements, standards, tariffs, and taxes are on a long list of subjects that influence S&T beyond simply funding. At the same time, the nation's dependence on technology to undergird economic health and security remains a significant fact of life.

A host of bedrock attributes of science and technology are also unchanging, often ignored, and often misunderstood. Some are clichés and some not so obvious.

First, all technologies are dual-use. There is no such thing as a technology that cannot be used for evil or malign purposes. Some are closer to weapons, but all of them have that capability. We have to recognize that the S&T enterprise inevitably produces more technology-based threats.

Second, the direction of technological development tends toward reducing the cost of performing a given function, thus contributing to the acquisition of dangerous technological capability by poorer countries or non-state actors.

Third, technological knowledge inevitably spreads. Diffusion can be delayed, but not prevented. The availability of a technology is only one part of a complex process that determines the potential for

misuse; and eventually all technologies will be available to those with the resources to use them.

Last, often the most significant applications of a new technology are far from the original purpose for which the technology was developed. You cannot predict precisely in advance how technology will develop or what synergisms among technologies will produce new applications.

What Has Changed For the Research Universities?

The most obvious change is the growth of large systems on which the economy and society have come to depend. Large systems mean large vulnerabilities. You can protect a system, reduce its vulnerability, and create redundancy, but you cannot remove vulnerability entirely. Society is simply too large and complex.

Another change is that the broader elements of science and technology necessary for our nation's security now cover a much wider range of subjects.

Yet another development is the expansion of the dimensions of size, distance, and power in the applications of technology. That obviously contributes to the phenomenon of globalization that characterizes the modern world.

Finally, a closer relationship between the laboratory and the marketplace (or application) means that more technologies are science-based. This makes scientific information itself a greater concern in terms of its potential for misuse.

Within the universities, much has changed. Most research universities are prospering, with more resources, increased endowments, and greater public support. At the same time, internationalization is becoming a much more common pattern among research universities. They are educating more foreign students, and carrying out many more foreign programs. There are a great variety of collaborations with people and institutions abroad and more contact with foreign corporations. At the very time we are concerned about threats from abroad, universities are actually expanding their international activity.

Obviously, part of the internationalization has been the growth of the numbers of foreign students and foreign scholars at American universities. The latest figure is close to 550,000 students, an increase

of 35 percent in 15 years. Sixty percent of these are in science and engineering, including the health fields. More than 50 percent of engineering doctorates and 25 percent of science doctorates are awarded to foreign nationals. Of course, foreign students and scholars contribute to the quality and the output of research. In fact, in some departments in the universities, there would be no educational or research function without foreign students. And foreign students tend to pay full tuition, which is not unnoticed. In addition, industry in the United States has come to depend on them. Foreign students, scholars, and researchers are vital to the advancement of science and technology in the United States and vital to our economy.

The universities have been largely free to determine their own policies toward foreign students and scholars. The federal government has control of the process only through visas. But, the Immigration and Naturalization Service cannot find three million people on student visas who they think have overstayed their welcome.

Another striking development in the universities is the closer ties to the private sector. This is not a new development, but it is growing.

Putting all of this together, I think we may have serious trouble ahead, and time is short. Obviously, the universities are moving in one direction, toward greater internationalization while jealously guarding the essential openness of the campus. At the same time our national concerns about proliferation, movement of information, and access of foreign students are intensifying in the opposite direction.

How Should We Respond?

This question is not easy to answer. It is imperative that the universities understand what the issues are, how they believe they should respond to them, how far they should go in accepting certain restrictions, and how they should work with government on these matters. I think it would be most unfortunate to wake up one day and, without warning, find legislation mandating restrictions on universities and foreign students.

Four prime areas need a response. One is the subject of openness, which must not be compromised. We may have concerns about the movement of information outside of the country or to people we wish did not have it. But that is not a problem that can be "solved."

We may, however, need to have new rules making it harder for certain information to be easily published. An example would be a handbook for designing weapons of simple kinds. These rules could be designed by the universities themselves, or by some kind of mandate, or preferably, worked out jointly by the universities and government. We are on a slippery slope here, but it may be necessary. We are never going to solve this problem completely, but we must at the same time be careful not to overreact.

The second issue is the relationship of our universities to foreign universities and corporations. Because of the close relations, there easily could be substantial concern that universities are providing too much information and too much access to foreign corporations. We went through this in the early 1990s with a very different set of issues. We wondered then if we were giving too much information and access to Japan. In the 1980s, it was with the Soviet Union on a different set of grounds. We must be careful to resist any formal restrictions that would force discrimination within the university community as to whom we can and cannot talk to concerning unclassified, open information.

A third area requiring response will be requests for the universities to use their capabilities for work that is related to terrorism. In the past, we had classified work done on campus to which only some people had access. If it is necessary to use the capabilities of the universities, as I am sure it will be, then any work that has to be secured through classification ought to be done away from the educational enterprise, off campus. It should not involve students, and perhaps only some of the faculty. To create a situation on the campuses where there were two categories of knowledge and two categories of access would be a most unwise step.

Lastly, the presence of foreign students adds a final area that will be threatened. One dimension will be an attempt to impose contractual restrictions barring foreign students from non-NATO countries from working on government-funded R&D. Such proposals have already been made, and clearly have to be resisted.

Another dimension is that of excluding individuals from a wide range of countries altogether. Denying entry to nationals from particular countries is a federal government responsibility through the visa process, not a university responsibility.

A third dimension will be requests to universities to monitor and report on foreign students. That is a difficult one and quite distasteful. I personally think that universities should not accept that responsibility on their own. If they are subpoenaed and it is a legal requirement, then they have to accede. Routine monitoring as to whether students are there and registered and whether they are following the course that they registered for is not a problem. But more extensive monitoring would be.

Conclusion

Can traditional values survive? I say they can, but it is a qualified yes, with considerable uncertainty. The dangers to the nation's security are obvious and very real to all of us. If we are not careful, it would not be hard to damage the resource the universities represent. This resource is critical for the strength, vitality, *and* the security of our nation.

Endnote

1. International Traffic in Arms Regulations (22 CFR 120-130), March 2001, § 120.9