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.