107th Congress
2nd Session

COMMITTEE PRINT

S. PRT.
107–61

TECHNOLOGY ASSESSMENT IN THE WAR ON TERRORISM AND HOMELAND SECURITY: THE ROLE OF OTA

REPORT

PREPARED AT THE REQUEST OF

HON. ERNEST F. HOLLINGS, *Chairman*

FOR THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

APRIL 2002

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE
78–705 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia
BARBARA BOXER, California
JOHN EDWARDS, North Carolina
JEAN CARNAHAN, Missouri
BILL NELSON, Florida

JOHN McCAIN, Arizona
TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia

Kevin D. Kayes, *Democratic Staff Director*
Moses Boyd, *Democratic Chief Counsel*
Jeanne Bumpus, *Republican Staff Director and General Counsel*

CONTENTS

LETTER OF TRANSMITTAL

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC, April 11, 2002.

DEAR COLLEAGUE: Technology is crucial to our conduct of the War on Terrorism and to the success of our homeland security programs. The Committee on Commerce, Science, and Transportation is deeply engaged in evaluating policies and programs involving the role of technology in enhancing homeland security in the areas of communications, airlines and airports, seaports, railroads, trucking, transportation of hazardous materials, manufacturing facilities, and science and technology in general. In conducting these evaluations, the Committee is concerned not only with the effectiveness and costs of the technologies, but also with their impact on U.S. industries and consumers, and the privacy rights of individual citizens.

To aid the Committee in its consideration of these matters, I have requested that a study conducted by Mr. Ellis R. Mottur, as a Public Policy Scholar at the Woodrow Wilson International Center for Scholars, be made available to the Committee. Mr. Mottur earlier served as the first Assistant Director of the Congressional Office of Technology Assessment and more recently as Acting Assistant Secretary of Commerce and Deputy Assistant Secretary for Transportation and Technology Industries.

This document contains the report prepared by Mr. Mottur, entitled: "Technology Assessment in the War on Terrorism and Homeland Security: The Role of OTA." Although the report has not been considered or endorsed by the Committee or any of its members, I believe it will be of interest to the Congress and many persons in the scientific, technical, academic, and professional communities, as well as the general public. To insure its general availability, I have directed that this document be published as a Committee print.

Sincerely,

ERNEST F. HOLLINGS,
Chairman.

LETTER OF SUBMITTAL

WOODROW WILSON INTERNATIONAL CENTER FOR
SCHOLARS,
Washington, D.C., March 22, 2002.

HON. ERNEST F. HOLLINGS, *Chairman,*
Committee on Commerce, Science, and Transportation,
U.S. Senate, Washington, D.C.

DEAR MR. CHAIRMAN: Thank you very much for your kind letter expressing interest in my study at the Woodrow Wilson Center. In response to your request, I am pleased to provide the Commerce Committee with my report entitled: "Technology Assessment in the War on Terrorism and Homeland Security: The Role of OTA."

The report focuses on the utilization of technologies in achieving homeland security, demonstrates the need for technology assessment to evaluate those technologies, traces the history of OTA, and concludes with a recommended course of action. I hope the report proves useful to the Committee.

With best personal wishes.

Sincerely,

ELLIS R. MOTTUR,
Public Policy Scholar.

Enclosure

PREFACE

In the months since September 11, it has become abundantly clear that America's unparalleled superiority in technology is critical to achieving success in the War on Terrorism and ensuring homeland security. Accordingly, the choices the United States makes with respect to the implementation of particular technologies will continue to be of paramount importance to the course of that struggle for years to come.

Those choices are exceedingly complex, involving assessments of effectiveness, costs, benefits, and impacts on the economy, environment, society, and human values, as well as comparisons with alternative technologies. Technology assessment is the methodology for making such choices.

As one of the founders of the congressional Office of Technology Assessment (OTA), and its first Assistant Director, I was well acquainted with that methodology and its application within the congressional context. Accordingly, in order to contribute to the national response to this unprecedented challenge, I joined the Woodrow Wilson Center as a Public Policy Scholar to conduct a study on technologies in the War on Terrorism and homeland security, with a focus on the potential role of OTA. The initial result is this report, which I hope proves useful in helping empower Congress to fulfill its legislative, appropriation, and oversight responsibilities in this overarching conflict.

I want to take this opportunity to express my gratitude to the Woodrow Wilson International Center for Scholars and especially to Michael Van Dusen, Samuel F. Wells, Jr., Kent H. Hughes, and Robert S. Litwak for making this project possible, to all of the Scholars at the Center for their stimulating intellectual discussions, to my intern, Jonathan Radke, for his valuable assistance, and above all to Lee H. Hamilton whose far-sighted, inspired leadership of the Center makes it as great a pleasure as it is a privilege to be a part of it.

Of course, the statements, views, and recommendations expressed in this report are solely the responsibility of the author and are not in any way intended to reflect those of the Woodrow Wilson Center, its management, staff, or other scholars.

EXECUTIVE SUMMARY

FINDINGS

- Technology is critical to U.S. success in the War on Terrorism and ensuring homeland security.
- A wide variety of sophisticated technologies may be involved in those efforts.
- Choosing among possible technologies and patterns of implementation is a complex process, oftentimes involving unintended consequences.
- Technology Assessment is the methodology for making such choices.
- The leading exemplar of technology assessment was the congressional Office of Technology Assessment (OTA), founded in 1972.
- For almost a quarter of a century, OTA provided Congress with valuable analyses of policy options on important issues involving technology.
- During that period OTA achieved a world-wide reputation for excellence, as a non-partisan, objective, and credible conductor of technology assessments.
- When OTA's funding was discontinued in 1995, there was no dissatisfaction with its performance; indeed OTA received accolades for its excellent work.
- Elimination of its funding was a cost-cutting measure at a time of fiscal stringency and a symbol for Executive Branch agencies to emulate.
- Congress now needs its own source of non-partisan, objective technology assessment in order to fulfill its legislative, appropriation, and oversight responsibilities in the War on Terrorism and ensuring homeland security.
- While OTA's funding was discontinued, its enabling statute remains in effect, including its authorization of "such sums as may be necessary."

CONCLUSION

To fulfill its constitutional responsibilities in pursuing the War on Terrorism and ensuring homeland security, Congress urgently needs to reactivate OTA.

RECOMMENDATION

In the first supplemental appropriation bill considered in this session, Congress should include $1 million for OTA to canvass and consult with congressional committees, and plan a series of technology assessments designed to meet the priority needs of those committees with respect to the War on Terrorism and homeland security.

RATIONALE

In the War on Terrorism, America's principal advantage is its unparalleled technological superiority—measured not only in highly sophisticated hardware and software—but also in the competence and character of its citizens in controlling that technology. This is true not only in dealing with the war, but just as importantly, in ensuring homeland security.

Terrorist Technology Threats

Each terrorist threat or act can be characterized by the specific technology utilized, by its means of delivery, and by its intended target. The diversity of technologies involved is enormous. There are 36 deadly biological agents, including 13 viruses, 7 bacteria, 3 micro-organisms with traits common to both bacteria and viruses, 1 fungus, and 12 biological toxins. Cyber-terrorists can hack into information systems, deny service to others by overwhelming sites with bogus requests, and spread computer viruses or worms. Chemical agents encompass nerve gases, cyanides, phosgene, and vesicants. Explosives run the gamut from nuclear fission, fusion, or dirty nuclear bombs through plastic explosives, nitrogen-based varieties, to pipe bombs, or simple hand grenades.

Similarly there are a great variety of means whereby terrorists can deliver their agents of destruction or disruption, including mail, modems, missiles, aircraft, ships, trains, trucks, autos, on foot, or by remote detonation. And their targets are equally varied, including: transportation and telecommunications systems; air, water and food supplies; energy sources and distribution channels; financial and computer networks; factories; key buildings; population groups; and prominent individuals.

But surpassing the extensive array of technologies, transmissions, and targets available to terrorists is the wide range of countervailing technologies we can deploy to deal with their threats or attacks. These fall into 3 categories, those aimed at: (1) precluding or deterring the terrorist act; (2) detecting it when it occurs; and (3) coping with its consequences.

Precluding or Deterring Terrorist Acts

The overarching campaign in this category consists of the current and projected military actions, along with the coordinated diplomatic, intelligence, public safety, and financial efforts to thwart terrorism wherever it lurks. On the homeland security front, there are a wide variety of technological systems under consideration. A number of these involve the enhanced coordination of more sophisticated, computerized information systems to track and apprehend terrorists before the deed is done. Most of the other technological systems directed at preventing terrorist acts are aimed at either or both of 2 goals: (a) to maintain boundaries which only authorized individuals can traverse; and (b) to ascertain whether the identities of specific individuals or entities meet the authorization criteria. The role of technology in maintaining boundaries lies essentially in electronic barriers, surveillance sensors, video cameras, alarms, and communications systems.

Identification technologies to confirm authorization to traverse boundaries include those aimed at screening things and those designed to verify persons' identities. Since conventional x-ray screening of baggage is not very effective for moderately sophisticated explosive devices, a number of more advanced systems are being investigated, such as pulsed fast-neutron transmission spectroscopy. An example of a technology for screening things that may be carried by persons is a holographic imaging system that can see objects hidden under clothing. A host of new technologies are being studied for verifying individuals' identities, including sophisticated biometric identification techniques, such as facial pattern recognition and iris or retina scanning systems.

Detecting Terrorist Acts When They Occur

If the terrorist act involves an explosion or shooting, witnesses are immediately aware that something terrible has transpired; but if the act involves cyber-terrorism or chemical or biological agents, there may be a considerable time lag before the act is discovered. If cyber-terrorists disrupt major electric power or communications systems, the act would be readily recognized; but when cyber-terrorists introduce computer worms or viruses into information systems, crucial time may elapse before the deed is discovered. Detection of chemical or biological agents is even more challenging. An example of a detection technology under development is a portable isotopic neutron spectroscopy chemical assay system that can identify nerve gases or explosives. Detection of biological agents is most difficult since the effect on the exposed individuals may not become apparent for a considerable period—by which time it may be too late to counteract the agent. An example of a technology being considered for detecting 8 different biohazards (including anthrax spores) is Polymerase Chain Reaction of PCR which uses specific enzymes to amplify tiny quantities of DNA to match them with DNA samples of the biological agent.

Coping with the Consequences of Terrorist Acts

After a terrorist act has been detected, it is imperative that its nature and extent be rapidly comprehended so that appropriate countermeasures can be undertaken. But it is sometimes difficult quickly to ascertain the character of chemical agents utilized in an attack; and biological weapons are especially troublesome in confounding rapid comprehension of what has transpired, as was evidenced in last fall's anthrax attacks. To facilitate more rapid comprehension, there's a need for a greatly improved communications network. This is underscored by the fact that the Centers for Disease Control (CDC) were not aware of May 2001 Canadian studies that confirmed the threat of spreading anthrax through the mail, even though 6 other U.S. agencies were cognizant of the studies. CDC did not learn of the studies until early November when the anthrax outbreak was almost over. Examples of technologies for coping with chemical attacks are the Antidote-Treatment-Nerve-Gas-Agent Auto-injector, a pen-like device to administer both types of anti-nerve-gas antidotes, and Sandia National Laboratory's development of a nontoxic, non-corrosive foam to neutralize chemical agents. Examples with respect to biological agents include an advanced, hand-held nucleic acid-analyzer to identify biological agents in the field within a matter of minutes and the use of irradiation of mail to destroy bacteria or spores. The administration's budget includes $6 billion for combating bioterrorism, including a substantial amount for research and development of such technologies.

Technological Choice

Choosing among the vast array of technological options for homeland security is a complex process. Sometimes there are inadequate data; other times the underlying science is not fully understood. But even when the scientific basis and data are available, there remains the so-called 'Law of Unintended Consequences,' which refers to the fact that many technologies engender ancillary, unexpected consequences that are difficult to foresee and sometimes detrimental in their impacts.

The most obvious example from the past is the use of the internal combustion engine for vehicles. While this innovation served as one of the prime movers of 20th century economic expansion, its long-term effects on the environment have been deleterious because of air pollution and the possibility of global warming. Another example is the use of chlorofluorocarbons for refrigeration and air conditioning. Along with the very beneficial effects of this innovation has come the diminution of the ozone layer, which serves to block the sun's rays and prevent skin cancer.

The point of these past examples is not that we should have refrained from utilizing the internal combustion engine for vehicles or Freon for cooling, both of which have bestowed substantial benefits on our standard of living. But if we had anticipated their ancillary, adverse consequences earlier, we might have been able to structure their implementation in such a way as to mitigate those unintended consequences and to design research and development programs aimed at alternative or supplemental means of achieving the same ends.

Technologies considered for homeland security have already exhibited some unintended consequences. The irradiation of mail damages computer chips, film, food, pharmaceuticals, contact lens, etc. Moreover, the process appears to have caused illness in some mail handlers because the irradiation heats the plastic warp used to protect the mail, thereby releasing noxious fumes. A potential problem arises with retinal scanning for identification purposes because of possible adverse health effects from the infrared light used to scan the retina and the threat of infection because of contact with the equipment. With respect to on-flight security, it appears that Tasers, a kind of stun gun, might interfere with the plane's operational instruments. A broader case of unintended consequences involves the impact on personal privacy from the more intrusive use of surveillance cameras and the integration of data bases containing background information on individuals. Similarly the wider use of antibiotics, like Cipro, could trigger greater resistance as bacteria adapt to them. The planned computerized, surveillance system of foreign students has also engendered considerable opposition from the colleges and universities that fear the loss of their tuition—another unintended consequence.

The lesson from all this is that technologies often have unintended, ancillary consequences which—to the extent feasible—

should be anticipated and taken into account in selecting among alternative technological solutions and structuring their implementation. The point is not that any particular technology is inherently good or bad, but rather that its relative benefits and detriments depend partially on its ancillary consequences, as well as on the uses to which it is put and the way in which it is implemented.

Technology Assessment

The analysis, comparison, and selection of technologies is a complex process, involving the following components:

- determining the technical capabilities of the technology;
- evaluating its effectiveness in achieving its primary objectives;
- ascertaining its costs;
- delineating the benefits it confers;
- anticipating its ancillary consequences, both positive and negative;
- discerning its probable impact on the economy, environment, society, and individual values;
- comparing the technology with alternatives in terms of all the foregoing factors; and
- delineating the advantages and disadvantages—the pros and cons—for the various policy options confronting decision makers.

Technology assessment is the methodology for conducting such analyses. Incorporating elements of operations research, systems analysis, cost-benefit studies, game theory, linear programming, simulation studies, and alternative-futures scenarios—along with pragmatic public policy considerations—technology assessment emerged as a distinct field of academic research in the mid-1960s. After 5 years of extensive hearings before the House Science and Astronautics Committee, and subsequent consideration by the Senate Rules Committee, the Technology Assessment Act of 1972 was signed into law on October 13, 1972, thereby establishing OTA as only the third support agency of Congress in the history of the Republic. (The Congressional Budget Office (CBO) was not created until 1974.)

During the legislative consideration of creating OTA, a great deal of attention was focused on why Congress needed a new agency, rather than relying on CRS and GAO. It was the overwhelming judgment of the academic, scientific, technical, and public policy communities that neither CRS nor GAO was capable of carrying out the technology assessments required by Congress, a view in which the Director of CRS, the Librarian of Congress, and the Comptroller General all concurred.

OTA went through its formative stages, guided by its Founding Director, former Congressman Emilio Q. Daddario. OTA later achieved maturity under the leadership of Director John Gibbons, who served about 15 years from 1979 to 1993. He built the credibility of the Office within Congress and throughout the nation's academic, scientific, technical, and professional communities. Indeed, OTA was recognized worldwide as the top institution of its kind, with many countries creating their own comparable organizations, modeled on OTA, including Austria, Denmark, the European Union, France, Germany, Great Britain, the Netherlands, and Sweden. While OTA products had a pervasive impact on congressional activities during the Gibbons Era, and the Office received many accolades and awards, its impact was best summed up by an article in the Federal Times, which stated: "[I]n a town where unimpeachable sources are oh-so-hard to come by, OTA has managed to secure a position near the top of the list." [1]

OTA's Structure and Pattern of Operations

OTA consists of a congressional Technology Assessment Board (TAB), a Director and his staff, and an Advisory Council. TAB consists of 6 Senators and 6 House members, evenly split between the 2 parties. The 10 public members of the Advisory Council are appointed by TAB and are joined on the Council by 2 ex officio members, the Comptroller General and the Director of CRS. TAB appoints the Director, who then appoints the office staff. The TAB Chairmanship rotates between Senate and House in different congresses. Traditionally the Chairman comes from the majority party in his House and the Vice Chairman from the opposite party in the other House. Assessments are undertaken at the request of congressional committees, not in response to individual members as is the case with CRS and GAO.

For each assessment undertaken, OTA convenes an advisory panel made up of experts, stakeholders, and citizens relevant to the particular assessment. These advisory panels play a key role in the design of the assessment, in the analysis of the data that has been assembled, and in reviewing the final report, which is also examined by a number of other outside reviewers who bring special expertise and points of view to the assessment. Over time OTA came to draw upon a pool of about 1,000 panelists and outside reviewers.

The overall assessment process embodies a series of checks and balances that confer credibility, objectivity, and relevance on the final report. Some of the most important checks and balances are the:

- even balance between House and Senate and the 2 parties on TAB;
- tradition of the Chair and Vice Chair from opposite parties;
- need for TAB approval to initiate assessments and release reports;
- Advisory Council's salutary influence on OTA's standards of excellence;
- advisory panel's role in design, analysis, and review of assessment;
- role of stakeholders and additional outside reviewers;
- preparation of Review Memorandum which describes reactions of panelists and reviewers to each portion of report and shows how final version takes account of those comments; and

- the pattern of continuing, informal communication between OTA and committee staff before, during, and as follow-up to the assessment.

With this understanding of the OTA process, it becomes clear why neither CRS nor GAO could effectively carry it out. Neither one operates under the close control of a congressional board; neither one responds only to requests from committees; and neither one has the statutory authority or institutional capability to integrate the expertise and views of 1,000 outside advisers into assessments.

Examples of some OTA reports particularly relevant to the War on Terrorism and homeland security include:

- *The Border War on Drugs*
- *Electronic Surveillance in a Digital Age*
- *High Level Radioactive Waste Site Characterization*
- *Impacts of Antibiotic-Resistant Bacteria*
- *New Developments in Biotechnology*
- *Scientific Validity of Polygraph Testing*
- *Taggants in Explosives*
- *Technology Transfer to China*
- *Technology and Counter Terrorism*
- *Transportation of Hazardous Materials*
- *Virtual Reality and Technologies for Combat Simulation*
- *Technologies Underlying Weapons of Mass Destruction*

OTA: 1993–1995

After about 15 years of outstanding service, Gibbons resigned as OTA Director in early 1993 to join the new administration. He was succeeded by Dr. Roger C. Herdman who had been serving as Assistant OTA Director with responsibility for Health and Life Sciences.

In 1995, however, there was a sea change in control of Congress. The new leadership was intent on eliminating a number of cabinet departments and on reducing the costs of government, including within the Legislative Branch. The likeliest target for reduction within Congress was one of the support agencies, CBO, CRS, GAO, and OTA. Of these, OTA was the smallest and most vulnerable. Accordingly, in order to save money, the House Appropriations Committee recommended elimination of all funding for OTA. This was strenuously opposed by many members—including all TAB members in the House—but the leadership prevailed. In the Senate the committee proposed a small amount for OTA, but only enough to enable it to close down its operations in an orderly manner. Again there was a strong effort to provide adequate funding, led by all Senators who have served on TAB. But again the majority voted it down and OTA ceased operations at the end of FY 1995.

Current Situation

As noted in the Findings, while OTA's funding was discontinued, its enabling statute remains in effect, including its authorization of "such sums as may be necessary." Moreover, since the Senate is a continuing body and the act does not limit the tenure of its members, the Senators who were Board members in 1995—Senators

Grassley, Hatch, Hollings, and Kennedy—are still Board members. Since the House is not a continuing body, it could be argued that the current House members who were on TAB in 1995—Representatives Dingell, Houghton, McDermott, and Oxley—would not still be members. But in any case, the act stipulates that: "Vacancies in the membership of the Board shall not affect the power of the remaining members to execute the functions of the Board." In short, OTA has an ongoing authorization for appropriations, and TAB is empowered to submit a recommendation to the Appropriations Committees for such an appropriation.

To underscore the urgent necessity for reactivating OTA, one example of OTA's potential impact on the War on Terrorism and homeland security should suffice. The anthrax attacks last fall engendered considerable confusion and consternation among public health authorities, public safety officials, and policy makers throughout federal, state, and local government. There was great uncertainty on many matters, including the number of spores necessary to trigger inhalation anthrax in humans; but it was widely believed that 8,000–10,000 spores would be needed to cause inhalation or pulmonary anthrax. If OTA had been operational at the time, it could have brought a highly relevant 1993 OTA report to the attention of the public health authorities. The report entitled *Technologies Underlying Weapons of Mass Destruction* stated: "1,000 spores or less can produce fatal pulmonary anthrax in some members of an exposed population."[2] If this information had been readily available, it's conceivable that it even could have saved a life or—at the very least—afforded much better guidance to the public health authorities in designing their response to the crisis.

It is clear that Congress urgently needs to reactivate OTA, and that to do so, all that is required is inclusion of $1 million in the next supplemental appropriation. Considering that this $1 million would reactivate an Office that could aid Congress in evaluating the $38 billion the President has recently requested for homeland security, the $1 million amount does not seem unreasonable.

*   *   *   *   *

TECHNOLOGY ASSESSMENT IN THE WAR ON TERRORISM AND HOMELAND SECURITY: THE ROLE OF OTA

In the War on Terrorism, America's principal advantage is its unparalleled technological superiority—measured not only in highly sophisticated hardware and software—but also in the competence and character of its citizens in controlling that technology. The military action in Afghanistan was a striking demonstration of those assets.

Eight thousand mile bombing runs from the continental United States, tactical aircraft sorties from carriers in the Persian Gulf or Arabian Sea, targeting by satellites and Predator drone planes, real-time information displays, GPS-guided smart bombs—along with night vision and special forces providing laser guidance on the ground—enabled precision bombing that could penetrate cave entrances horizontally and explode underground with greater devastation than hundreds of dumb bombs in World War II or Vietnam.

In short, the awesome enhancement of our military capabilities through technology is apparent to all who tune in to CNN. But perhaps not as overtly obvious, yet promising to be as powerful and pervasive is the potential impact of technology on homeland security. This potential impact flows both from the technology utilized by the terrorists and from the technology we need to employ to deal with their threats.

Terrorist Technology Threats

Each terrorist threat or act can be characterized by the specific technology utilized, by its means of delivery, and by its intended target. Thus the catastrophe of September 11 utilized jet fuel as an explosive, delivered by means of fully-fueled, Boeing-757 and -767 aircraft, and directed at the World Trade Center towers. The subsequent anthrax events utilized highly refined, aerosolizable anthrax powder, delivered through envelopes in the mail, and aimed at Senate and media personnel. The ongoing bombings in Israel utilize plastic explosives, delivered by suicidal individuals on foot or in vehicles, and targeted at groups of innocent bystanders.

These current examples illustrate the diversity of technologies, means of delivery, and targets that terrorists may employ. The full range of possibilities is extremely wide. Thus biological agents could include—besides anthrax—small pox, plague, viral encephalitis, yellow fever, and Marburg virus. Examples of other agents that could be introduced through the food supply are botulism, salmonella, E. coli, and cholera. In fact, "the Centers for Disease Control and Prevention lists 36 classes of . . . potential weapons . . . [including] 13 viruses, 7 bacteria, 3 rickettsiae (micro-organisms that have traits common to both bacteria and viruses), 1 fungus and 12 biological toxins."[3]

Cyber-terrorists utilize the internet, software, and their extensive computer skills to hack into purportedly inaccessible information systems, to deny service to others by overwhelming sites with bogus requests, and to spread deleterious computer viruses or worms. In contrast with weapons of mass destruction, "cyber threats are considered weapons of mass disruption . . . Computer security experts . . . have begun seeing evidence of increasingly potent attacks by hackers . . . denial of service attacks [are] becoming more common and more disruptive . . . Attackers have also employed 'worms' . . . aimed at routers, which direct traffic throughout the internet . . . No computer on the internet is immune from denial of service attacks."[4]

Chemical agents encompass: nerve agents like sarin, tabun, soman, and VX gas; cyanides; phosgene; and vesicants such as sulfur mustard gas. Explosives run the gamut from nuclear fission or fusion bombs to dirty nuclear bombs (which disperse radioactive materials without a chain reaction) to highly energetic plastic explosives to nitrogen-based (nitramine) varieties like nitroglycerine to pipe bombs or simple hand grenades. Arson can be committed merely with a container of gasoline and some matches. And of course, determined terrorists can rely on simple weapons like automatic rifles, hand guns or—as we saw on September 11—even small box cutters.

While not as diverse as the wide range of technologies terrorists may employ, there are a number of means through which they can deliver their agents of destruction or disruption, including: mail; computer modems; missiles; aircraft (from crop dusters to Boeing 767s); ships (from huge tankers to small harbor craft); trains; trucks; automobiles; bicycles; on foot; by a hand hurling a grenade; or by remote detonation, which itself can be accomplished by a variety of methods.

For example, in the "early 1970s, IRA [bombs in the UK consisted of] . . . nails wrapped around a lump of plastic explosive and detonated simply by lighting a fuse. . . . [Their] time bombs . . . were . . . dynamite and commercial detonators . . . attached to ordinary battery-powered alarm clocks." Later on to avert danger to their agents, they began detonating remotely "by using the radio controls for model aircraft. The British Ministry of Defense (MoD) thwarted this means of attack through electronic countermeasures and jamming techniques." The IRA then developed a "network of sophisticated electronic switches [to] bypass the . . . countermeasures . . . [T]he MoD scientists . . . [then devised] a new system of electronic scanners able to detect radio emissions . . . before the bomber can actually transmit the detonation signal." But the IRA subsequently developed "a photo-flash 'slave' unit that can be triggered from a distance of up to 800 meters by a flash of light."[5] So the various technologies for detonating and thwarting detonation continue to contend with each other.

The targets terrorists may attack are equally varied, ranging from: telecommunication systems; computer networks; water systems;[6] food supplies; energy sources and distribution systems (nuclear or coal power plants, hydroelectric dams, natural gas pipelines, oil refineries, etc.); transportation systems (roads, rail, subways, bridges, tunnels, seaports); financial institutions and networks; factories; key buildings; and concentrated populations or even prominent individuals.

The vulnerability of the nation's electric power system, for example, was underscored at a recent conference of industry executives, at which it was revealed that: "The computers that control the electric power system around the nation have been probed from the Middle East, and terrorists may have inspected the physical equipment . . . Government experts identified nuclear power plants as perhaps the most attractive targets, but said dams, gas pipelines and oil refineries were not far behind."[7]

Surpassing the extensive array of technologies, transmissions, and targets available to terrorists is the wide range of countervailing technologies we can deploy to deal with their threats or attacks. These countervailing technologies fall into three categories, those aimed at: (1) precluding or deterring the terrorist act; (2) detecting it when it occurs; and (3) coping with its consequences. It is instructive to examine illustrative examples of technologies in each of these categories.

Precluding or Deterring Terrorist Acts

The best example in this category, of course, is the current effort to root out and extirpate the Al Qaeda network, cells of which are reputed to be festering in about 60 countries throughout the world. Accomplishing this goal would surely go a long way toward precluding many terrorist attacks. But as President Bush reiterated in his January 2002 State of the Union speech, the War on Terrorism extends far beyond the Al Qaeda network or the former Taliban government, as is evidenced by the recent incursion of American special forces into the Philippines and planned deployments into Yemen and the Republic of Georgia. Furthermore, underscoring his oft-stated warning that nations that harbor terrorists are equally culpable, he specifically cited Iran, Iraq, and North Korea as "seeking weapons of mass destruction," castigating them as constituting "an axis of evil."[8] Proceeding in parallel with the military actions in Afghanistan and the Philippines and the President's public exhortations, are the coordinated diplomatic, intelligence, public safety, and financial efforts to thwart terrorism wherever it lurks. Undoubtedly this concerted campaign has already impeded previously plotted terrorist events.

But as President Bush also noted in his State of the Union address: "Thousands of dangerous killers . . . are now spread throughout the world like ticking time bombs, set to go off without warning."[9] To intercept and prevent any of their attempted terrorist acts from implementation, homeland security measures may encompass a wide variety of technological systems. Many of these technologies involve "the use of powerful computers . . . [which] can spot linkages among [innumerable] individual pieces of information . . . Germany pioneered the use of computers in this field . . . Two apparently unrelated individuals could be shown to be extremely likely to belong to the same terrorist group by showing an overlap in the information about them which was too complete to be coincidental . . . The FBI has now refined and expanded upon the capacities pioneered by the German police . . . [by developing a computer system] designed to draw investigative inferences from the organized examination of all the data that the Justice Department and its component agencies are collecting."[10]

Most of the other technological systems directed at preventing terrorist acts are aimed at one or both of two goals: (a) to maintain some kind of boundaries which only authorized individuals or entities can traverse; and (b) to ascertain whether the identities of specific individuals or entities meet the authorization criteria.

The boundaries can be as wide as the U.S. seacoasts and northern and southern border or as narrow as the walls of a particular facility, building, or secure room within a building. They can be the perimeters of nuclear, electrical, or telecommunications facilities or the confines of a particular airfield, airplane, seaport, ship, train station, train, bridge, or tunnel. They can be secured through appropriate configurations of powerful walls, fences, doors, electronic barriers, surveillance sensors, video cameras, communication systems, alarms, guards, and guard dogs. Current examples range from the projected increase of customs agents and immigration officials to be stationed at the Mexican and Canadian borders and various airports and seaports to the National Guard troops at nuclear power facilities to the reinforced cockpit doors on aircraft.

With respect to border crossings, a number of technologies are being explored. The Director of Homeland Security, Governor Tom Ridge said: "experimental high-tech 'fast lanes' for frequent travelers, and inspecting cargo trucks and electronically sealing them at locations away from the border would . . . move the border into the 21st century . . . [although] scanners to read the 5 million 'laser' identification cards issued to people who frequently cross the border [still need to be installed] . . . The new laser IDs include biometric features, such as fingerprints . . . The other new technology under discussion includes more mobile x-ray units, which resemble a drive-through car wash. A vehicle crossing the border would drive through the apparatus and an inspector could, for instance, detect false compartments used to smuggle people or check sealed cargo."[11]

The role of technology in maintaining boundaries lies essentially in electronic barriers, surveillance sensors, video cameras, communication systems, and alarms. Some examples will serve to illustrate the range of technologies involved. Thus alarm systems are generally based on hard-wire lines, microwave, radio frequency, or cellular transmission technologies.[12] When available, fiber optics may replace copper hard-wire lines, since fiber optics provides longer distance transmission and freedom from electromagnetic or radio frequency interference.[13] Because of the heightened emphasis on anti-terrorism activities since September 11th, many efforts are underway to develop more sophisticated surveillance systems. A good example is the software that has been developed by NetTalon Security Systems, Inc. of Fredericksburg, Virginia. This software enables real-time, simultaneous transmission to and from an aircraft and the ground for a host of video, sound, and sensor information (e.g., motion or vapor detection, changes in pressure or temperature, etc). As a result, the ground station could instantaneously trigger response mechanisms like aiming a Taser stun gun or releasing pepper spray at a precise target.[14]

Identification technologies to confirm authorization to traverse boundaries fall into two classes: those aimed at screening things and those designed to verify persons' identities. In both cases there are a multitude of technologies entering into practice, under consideration, or still in research and development. Illustrative of these is the wide range of devices under consideration for baggage screening at airports. Conventional x-ray screening of baggage is not very effective at locating moderately sophisticated explosive devices.[15] Other technologies that have been studied for this purpose include: thermal neutron activation (TNA); automated neutron-source accelerator; elastic neutron scattering; pulsed fast-neutron transmission spectroscopy (PFNTS); photon activation; nuclear resonant absorption (NRA); fast-neutron associated particle (FNAP); dual energy x-ray systems; backscatter x-ray; coherent x-ray scattering; and dual energy x-ray computed tomography (CT).[16]

Numerous other technologies are being developed for screening things that may be carried by persons. For example, the Pacific Northwest National Laboratory (pNNL) in Washington State has developed a hand-held "device that uses ultrasonic waves to see inside of sealed containers, a holographic imaging system that can see objects hidden under clothing, and a polymer that detects nerve agents." [17] The Federal Aviation Agency (FAA) is "developing . . . electromagnetic devices for screening bottles and other containers . . . [for] detecting liquid explosives." Other devices, known as trace detectors, have been manufactured for "detect[ing] the residue or vapor from explosives on the exterior of carry-on bags and on electronic items, such as computers or radios," or even on shoes. Other trace detectors under development screen items handled by persons to detect residue or vapor from explosives on the persons' hands. Also in development are walk-through screening portals that can: "detect particles and vapor from explosives on passengers' clothing or in the air surrounding their bodies." [18]

There is also a wide array of technologies being considered for verifying individuals' identities and authorization to traverse boundaries. Some of these are as simple as the use of wireless devices with software developed by Aether Systems, Inc. of Maryland whereby airport security personnel can instantaneously check electronic records to identify passengers, airport employees, and vehicles.[19] Others include the more extensive use of photo IDs and smart cards (with embedded computer chips), encryption for electronic communications, and increasingly sophisticated biometric identification techniques. One biometric system utilizes passive and active imaging technologies, which "can see through clothes and produce an image of the human body underneath . . . In passive screening, the natural radiation emitted by the human body is detected and analyzed . . . Active imaging entails irradiating the body with x-rays or millimeter waves and analyzing the radiation scattered from the body . . . [M]etallic weapons or explosive materials . . . will appear different from [the body]." [20]

Generally, biometrics refers to a set of technologies that utilize human characteristics or behavioral traits to identify particular individuals. These include: fingerprinting, finger patterns, palm prints, hand geometry, hand topography, hand and wrist vein patterns, facial pattern recognition, voice recognition, signature or handwriting analysis, key stroke dynamics, and iris or retina scanning. An example that employs facial pattern recognition is the FaceIT technology manufactured by a New Jersey company, Visionics. This system generates ID codes "based on 80 unique aspects of [individuals] facial structures, like the width of the nose and the location of the temples. FaceIT can instantly compare an image of any individual's face with a database of the faces of suspected terrorists." [21] Iris scanning systems are based on the fact that not only are everyone's irises—even those of identical twins—different, but also that each individual's two irises are different from each other. Software has been developed that enables scanning and database comparison of irises to take place within a few seconds.[22]

Detecting Terrorist Acts When They Occur

When efforts to prevent or deter terrorism fail and a terrorist act occurs, it is not always immediately obvious what has happened. If the terrorist act involves an explosion or shooting, witnesses are immediately aware that something terrible has transpired; but if the act involves cyber-terrorism or biological or chemical agents, there may be a considerable time lag before the act is discovered. Our increasingly interdependent, technologically complex society is highly vulnerable to the disruptive effects of cyber-terrorism. If such acts were to penetrate and disrupt the FAA flight control system, or power grids, or major communication systems, they would undoubtedly be readily recognized. It also would be obvious if the method of disruption consisted of, "flooding [an information] system with false requests for service [so that it was] impossible to respond to legitimate requests"—as happened with Yahoo in the year 2000.[23] But if the hackers or cyber-terrorists cleverly introduce computer worms or viruses into information systems—as is occurring with increasing frequency[24]—prompt detection of the act poses a constant challenge to the ingenuity of our software designers and the vigilance of our system operators.

Detecting the introduction of chemical or biological agents is perhaps even more challenging. One of the most widely reported acts of chemical terrorism occurred on March 20, 1995, when "the nerve gas sarin was released in commuter trains on three different Tokyo subway lines by a terrorist cult group. Sarin was concealed in lunch boxes and soft-drink containers and . . . released as terrorists punctured the containers with umbrellas before leaving the trains. Over 5,500 were injured," 11 of whom died. Since there was no detection capability within the train system and since sarin is colorless and odorless, detection occurred only after sick patients flooded the area hospitals.[25]

To provide rapid detection for such events in the future, U.S. scientists from Argonne, Sandia, and Lawrence Livermore national laboratories "have been developing and experimenting with chemical sensors in two downtown [Washington] Metro stations . . . [They have] studied how air moves through the subway and how trains, heat and humidity affect air flow . . . how chemicals spread . . . [and how they] can be released through air exhaust systems into the streets above . . . They can detect the presence of a harmful chemical, such as sarin gas, [but] cannot yet detect biological agents, such as anthrax."[26] Other detection technologies under development at the national laboratories include: "a cyanide microsensor, [a] portable isotopic neutron spectroscopy chemical assay system that can identify nerve agents, compressed gases, or explosives inside artillery shells or bombs [and] . . . a 'laboratory on a chip' that can identify . . . all . . . known chemical warfare agents in under 30 seconds."[27]

Detection of biological agents is generally more difficult because the effect of the biological agent on the exposed individuals frequently does not become obvious until quite some time has elapsed; and oftentimes it is then too late to counteract the harmful agent. So it's imperative that effective detection technologies are developed and made widely available throughout the U.S. public health system.

Biological agents can be delivered through the air, the water, the food supply, or—as we recently witnessed—through the mail system. Since detecting biological agents in the mail poses extremely daunting problems, high security targets—like the Congress and key government agencies—are beginning to irradiate all such mail in an effort to kill any biological organisms that may be present.

The U.S. Postal Service recently announced its exploration of an even more sophisticated technology that could "detect eight biohazards, including anthrax spores." Termed PCR (for polymerase chain reaction)—although sometimes referred to as 'molecular photocopying'—the technology would take air samples every half-hour from mail passing through high-speed postal sorters and test the samples for the specific signatures of particular bacteria like anthrax. "PCR is a general term for a process that uses specific enzymes to amplify tiny quantities of DNA and make a DNA match."[28]

With respect to food, the current system for detecting contaminants is similar to searching for a needle in a haystack. The paucity of resources that have been devoted to this effort is thinly spread among the Departments of Agriculture, Commerce, and Defense, the Food and Drug Administration, and the Environmental Protection Agency. Inspections are infrequent and some items—e.g., fish that goes from the boat directly to a wholesaler or retailer—are not inspected at all. Moreover, "the Centers for Disease Control and Prevention catches [sic] only a small percentage of food-borne outbreaks because state reporting is voluntary and inconsistent." In 1984 when "members of a religious commune in Oregon contaminated 10 salad bars with salmonella [sickening] 151 people . . . it took a year to link the outbreak to the commune."[29]

With respect to biological agents in general, "because the time lag between exposure to a pathogen and the onset of symptoms may be days or weeks, effective response to a covert terrorist action will be critically dependent upon (a) the ability of individual clinicians, perhaps widely scattered around a large metropolitan area, to identify and accurately diagnose an uncommon disease and (b) a surveillance system for collecting reports of such cases that is actively monitored to catch disease outbreaks as they arise."[30]

One such surveillance system is the Pittsburgh "Real Time Outbreak and Disease Surveillance System [which] tracks patients by zip code, looking for spikes that often signal an upcoming wave of illness. For example, a jump in fever and respiratory illness in one neighborhood could tip off medical detectives that an anthrax outbreak has occurred."[31]

Unfortunately, the nation's public health system is woefully unprepared to deal effectively with bioterrorism. "Vast numbers of the nation's private doctors are uninformed about how to recognize, treat and report casualties of a biological attack."[32] "Half of all

U.S. states [lack] even a single 'disease detective' to investigate outbreaks . . . Ten percent of the nation's 120 largest city and county health departments [do] not have e-mail." [33] While "some serological, immunological, and nucleic acid assays are available for identifying . . . biological agents, . . . [since] laboratories do not perform these assays regularly . . . it therefore seems unlikely that many labs will be immediately prepared to conduct the specific analytical test needed . . . even when the attending physician is astute enough to ask for the appropriate test." [34] To begin to remedy these deficiencies in the nation's public health system, the President's recent budget calls for an increase in overall funding for combating bioterrorism to $5.9 billion, including "$1.2 billion to improve the ability of state and local health systems to respond to bioterrorism attacks." [35]

Coping with the Consequences of Terrorist Attacks

After a terrorist act has been detected, it is imperative that its nature and extent be rapidly comprehended so that appropriate countermeasures can be undertaken. Even with a simple explosive or shooting attack, one has to determine the number of fatalities and the nature and extent of the injuries. In the case of arson, one has to know the extent and nature of the fire to know where to deploy the firefighters and what type of extinguishers to employ. It is sometimes difficult quickly to ascertain the character of chemical agents utilized in an attack. But when dealing with a 'dirty' radiological device or a nuclear bomb, the process of comprehension becomes even more complex. While acts of cyber-terrorism can usually be traced to their sources, the challenge comes in doing so fast enough to minimize the damage they have caused. And biological weapons are especially troublesome in confounding rapid comprehension of what has transpired.

The recent anthrax attack illustrates the nation's lack of necessary knowledge and effective organization to deal with biological terrorism. First, there was widespread confusion within the public health system as to the nature of the anthrax involved and, indeed, the amount of anthrax needed to cause inhalation anthrax in humans. Moreover, while the mails were used to transmit the anthrax spores to Senator Daschle's office in October 2001, as of this writing in March 2002, there is still no resolution as to how anthrax was transmitted to the women who died in New York and Connecticut. Equally baffling is the case of the postal inspector who spent 45 days in a Baltimore hospital after inspecting a mail-sorting machine at the Brentwood facility in which the Daschle letter was processed. Although he evinced most of the symptoms of inhalation anthrax, there was no evidence of anthrax bacteria in his blood.[36]

Clearly there are three paramount preconditions that must be met in order to promote the more rapid comprehension of the nature and extent of terrorist acts: Firstly, we need much more research and development, especially regarding all aspects of bioterrorism. Secondly, we need much more extensive and effective educational programs for the front-line responders to terrorism (police, firefighters, emergency rescue teams, hazmat squads, etc.), as well as the medical and scientific public health officials who must analyze the situation and prescribe treatment. And thirdly, we need a vastly expanded and enhanced communication network integrating the intelligence community with state and local government officials, front-line responders, police and other public safety officers, and public health diagnosticians and practitioners.

The need for a greatly improved communication network is underscored by the fact that the Centers for Disease Control (CDC) were not aware of significant Canadian studies conducted in May 2001, "which showed . . . that a real anthrax threat letter was a far more dangerous weapon than anyone had believed . . . [Although] bioterrorism and civil defense experts in a half-dozen [U.S.] agencies had the information . . . CDC epidemiologists . . . didn't learn of the Canadian studies until early November. By then, the anthrax outbreak was almost over."[37]

Depending on the determination of the nature and extent of the terrorist act, there are a number of ways we can attempt to cope with its consequences. When cyber-terrorism has occurred, it is up to the experience, ingenuity, and software available to the cybersecurity experts to structure the best approach to blocking further damage and restoring the system under attack to its normal functioning. When the terrorist employs small arms fire or simple explosives, the treatment for non-fatal victims is straightforward, requiring the standard medical technologies for dealing with accident injuries. In addition, newly developed technologies can ameliorate the situation. For example, there is the jackhammer developed at Brookhaven National Laboratory "for rescue teams working in collapsed, unstable buildings. The jackhammer . . . creates fewer shocks and vibrations than a conventional device, reducing the risk of further collapse . . . [And Sandia National Laboratory is developing] the robot family, a group of intelligent, mobile machines that can swarm over a site . . . looking for victims . . . The robots . . . have demonstrated independent 'swarm intelligence' in carrying out their tasks."[38]

In cases when the terrorist has perpetrated arson, technology can be of great assistance in enhancing the effectiveness of the response. For example, the NetTalon system cited earlier with regard to internal aircraft surveillance could also be utilized in fighting fires. That system would enable the firefighters speeding to the scene to have real time pictures on their laptop screens of precisely where in the building the fire was located, its intensity, speed of spreading, associated vapors, and whether it required water or specialized foams.[39]

A rudimentary response to a chemical gas attack, of course, is to don a gas mask before the gas takes effect. "Although sarin [nerve] gas can seep through the skin, breathing it in delivers a lethal dose about 400 times faster—so the mask could give you enough time to escape from a noxious cloud." However, the mask has to be in good working order, and the fit has to be airtight for it to function effectively.[40] A good example of a technology for responding to chemical attack, is the Antidote-Treatment-Nerve-Gas-Agent Autoinjector developed by Meridian Medical Technologies, Inc. of Columbia, Maryland. This pen-like device enables soldiers to self-administer precise doses of both types of required anti-nerve-gas antidotes (atropine and praladoxime chloride).[41] Another excellent example is Sandia National Laboratory's "development of a nontoxic, noncorrosive foam that neutralizes both chemical agents and biologic species such as anthrax . . . The foam . . . was used extensively to clean up anthrax-contaminated areas on Capitol Hill." [42]

With respect to biological agents, Lawrence Livermore National Laboratory has developed a prototype of an advanced, hand-held nucleic-acid-analyzer, only slightly larger than a scientific calculator, that would enable emergency workers to identify biowarfare agents in the field in a matter of minutes.[43] For use after a dangerous substance has been detected, the same national laboratory has developed a gel "to kill biological agents and neutralize chemicals without harming people." [44] Another approach, still in the research phase, is the attempt to find an antitoxin that would neutralize the toxins produced by the anthrax bacteria. A group at Harvard Medical School led by Dr. R. John Collier has developed two methods of neutralizing the anthrax toxins: one by combining with the toxin molecules and inactivating them; the other by adhering to the toxin molecules and blocking them from entering the host cells. Both methods have been tested on rats who have survived with no symptoms. Still another approach, in an early research stage, "involves a new type of antibiotic against anthrax bacteria . . . discovered by Dr. Lucy Shapiro of Stanford University and Dr. Stephen J. Benkovic of Penn State. In early laboratory tests, this antibiotic worked not only against anthrax bacteria, but also against brucellosis and tularemia, both of which are "potential germ warfare weapons." [45]

An entirely different approach for counteracting biological agents is irradiation. But, of course, this cannot be used on infected individuals, but only on things that are carrying the bacteria or the spores that will produce the bacteria. Following the delivery of anthrax-laden letters to Capitol Hill in October, all mail for the White House and Congress and much of the mail for federal agencies is irradiated. All mail for Washington, D.C. is first machine sorted for zip codes. All mail with government-zip-code destinations is then sorted by hand. Mail for the White House, Congress, and much of the mail for other federal government entities is then "wrapped in plastic, packed in boxes, and taken by tractor-trailer to irradiation centers in Bridgeport, New Jersey or Lima, Ohio." At those centers the boxes of mail move on a conveyor belt past a 'gun' that subjects them to a high dose of ionizing radiation. Afterwards they are trucked back to Maryland where "they are opened and allowed to breathe for up to 48 hours to dispel gases created by irradiation." They are then ready for final sorting and delivery.[46]

Regardless of which technology is used to respond to the effects of the terrorist act, critical to the success of any countermeasures are the resources, training, and organization that are brought to bear on the situation. For example, in dealing with a chemical attack: "the removal of solid or liquid chemical agent from exposed individuals is the first step in preventing severe injury or death . . . Very few [hazmat] teams are staffed, equipped, or trained for mass decontamination . . . [F]ew hospitals have formal decontamination facilities; even fewer have dedicated outdoor facilities or an easy way of expanding their decontamination operations in an event involving mass casualties." [47] The administration's budget submission for FY 2003 makes a start toward remedying these deficiencies. The $38 billion for Homeland Security includes nearly $6 billion for combating bioterrorism, encompassing a range of programs: research and development for vaccines, diagnostic tests, decontamination methods, and related technologies; expansion of the National Pharmaceutical Stockpile; development of rapid response networks; and training and technical assistance to states and local governments to strengthen their public health systems.[48]

Technological Choice

It is clear from the preceding discussion that the menu of technological options available for homeland security is vast. However, choosing among alternative strategies and technologies is not a simple, straightforward matter; on the contrary, it is highly complex and fraught with difficulties. Sometimes there are inadequate data on which to base a sound decision; other times the underlying science on which the technology is founded is not fully known—as was the case with understanding the transmission of inhalation anthrax from anthrax spores.

Even when the scientific basis and data are available, however, a significant difficulty remains: the so-called 'Law of Unintended Consequences.' This refers to the historical fact that many technologies have engendered ancillary, unexpected consequences that are frequently difficult to foresee and sometimes somewhat detrimental in their impacts. In order to gain some perspective on this issue, it is useful to examine some examples from the past and some apparent instances that have already emerged in the application of technology to the War on Terrorism.

The most obvious example from the past is the use of the internal combustion engine to power automobiles and other vehicles. There is no question that this innovation served as one of the prime movers of 20th century economic expansion. Moreover, it not only facilitated much more rapid transportation of people and goods, but also its initial impact on the environment was salutary; for it led to the elimination of foul-smelling horse manure from roads and city streets. Yet we now know that its long-term effect on the environment has been deleterious because of its substantial contribution to air pollution and the possibility of global warming. Furthermore, the use of motorized vehicles has had the unfortunate ancillary consequence of tens of thousands of traffic fatalities and injuries in the United States annually.

Another past example of the 'Law of Unintended Consequences' was the use of chlorofluorocarbons for refrigeration and air conditioning. This was an immensely important innovation that facilitated the comfortable use of many otherwise unsuitable facilities in the heat of summer and the longer-term distribution and preservation of food products, thereby transforming the role of homemakers who no longer had to shop for food each day. In referring to Freon, a trade name for these chemicals, the 1973 edition of the Encyclopaedia Britannica stated: "The importance of the Freons lies in the fact that they are so stable that they are entirely harmless."[49] As we now know, however, it is the very stability of these chemicals that enables them to rise up above the atmosphere and serve to deplete the ozone layer, thereby interfering with its blocking of sun rays that can cause skin cancer.

The point of these past examples is not that we should have refrained from utilizing the internal combustion engine or making use of refrigeration and air conditioning; both innovations have bestowed substantial benefits on our standard of living. But if we had anticipated their ancillary, adverse consequences earlier, we might have been able to structure their implementation in such a way as to mitigate those unintended consequences and to design research and development programs aimed at alternative or supplemental means of achieving the same ends.

As noted above, some apparent instances of the 'Law of Unintended Consequences' have already emerged in the application of technology to the War on Terrorism. Most notable among them is the use of irradiation to sanitize mail from anthrax spores and other pernicious contaminants. This "process tends to destroy computer chips and to damage . . . delicate items including food, [photos], pharmaceuticals, clothing, contact lens—and even the paper mail itself."[50]

Also the fact that the process entails wrapping the mail in plastic prior to irradiation has apparently caused varying forms of distress among some mail handlers. This may be due to the interaction of the electrons [in the irradiation] and the plastic wrap, thereby producing ozone and carbon monoxide.[51] In any case, the mail room in the U.S. Department of Commerce had to be temporarily shut down because a number of the mail room employees complained of nausea and respiratory distress.[52] Similarly "seventy-three employees of the U.S. Senate have reported health problems including headaches, eye irritation and skin rash after handling irradiated mail, and the government has issued a cautionary advisory to 180,000 federal workers in the District.[53] In addition, "87 . . . workers at the Gaithersburg [Maryland mail] facility . . . are experiencing nosebleeds, runny noses, runny eyes, extreme headaches, nausea."[54]

Again these unanticipated consequences do not imply that sensitive mail should not be irradiated. Indeed, as a result of such concerns, "engineers lowered radiation dosages by about 40% after concluding that that was sufficient to kill anthrax spores and other biological contaminants."[55] Also mail is now being "removed from the boxes and plastic and allowed to air . . . for as long as 48 hours before re-entering the usual mail delivery system."[56] The point is that the earlier one can anticipate the ancillary consequences, the better one can implement the technology in a manner designed to obviate or mitigate its adverse effects.

An example of a potential problem with an identification technology occurs in the field of biometrics. "Retinal scan . . . is perhaps the most secure biometric option. Users, however, fear health effects from the infrared light used to read the retina, as well as possible infections from contact with the equipment . . . [Moreover,] a person's retinal patterns change after he or she experiences a heart attack. Unions have fought the installation of retinal scan equipment on the theory that the scan could be used by companies to spot sick employees and terminate them."[57] Iris scans may not be as reliable as retina scans, in terms of false acceptance or false rejection rates, but since they do not involve physical contact, they may prove more desirable in some instances.[58] This example illustrates the importance of including examination of ancillary consequences in consideration of alternative technologies.

Technologies for coping with terrorists who are onboard an aircraft in flight also pose a number of problems that need to be assessed, according to a draft report of the National Institute of Justice, a research resource of the Justice Department. The draft report stated that: "Tasers—a type of stun gun . . . could interfere with the plane's operational instruments . . . 'In the preliminary tests . . . an electrical discharge less-than-lethal device fired at cockpit instruments adversely affected a number of systems . . . [Furthermore,] in the confined space of a cockpit, crew members are likely to be incapacitated' . . . by other non-lethal weapons such as pepper spray or tear gas . . . [The draft report also raised serious questions on a number of other technologies, including,] . . . the Laser Dazzler, a light that temporarily blinds an attacker, . . . anesthetics or calmative chemicals that could incapacitate all passengers when released into the air, a 'slippery foam' on the cabin floors that could make an attacker slip, and some kinds of ear-piercing acoustic weapon."[59]

A broader problem of unintended consequences that permeates a number of the technologies that may be used in the War on Terrorism is their impact on the privacy of individuals. This impact can be readily perceived in the proliferation of video cameras and human scanning equipment for purposes of security. As indicated earlier, one biometric system utilizes imaging technologies that can penetrate clothing and produce an image of the body beneath them.[60] The increasing use of closed circuit TV (CCTV) for security surveillance portends a pervasive impact on personal privacy. The proliferation of CCTV in the UK over the past decade may be a prognosticator of what lies ahead for the United States. In the early 1990s, after terrorist bombs exploded in the 'City of London,' the government installed a network of CCTV cameras around that area and over the decade encouraged local governments to do the same in their areas. "By 1998, 440 city centers were wired [with CCTV] . . . There are now [estimated to be] 2.5 million surveillance cameras in Britain."[61] "In Britain in the late 1990s it is unlikely that any urban dweller, in their [sic] role as shopper, worker, commuter, resident or school pupil can avoid being . . . monitored by camera surveillance systems."[62]

A further instance of the potential invasion of privacy arises from the intended expansion and integration of data bases containing background information on individuals for use in security at airports, seaports, border crossings, etc. The more extensive and integrated such data bases are, the more susceptible they become to misuse of the information. A third example of the potential infringement of privacy comes from the pervasive expansion of the internet, with its manifold possibilities for mischief. As these technologies continue their diffusion, it is essential that every effort be made to ensure as much protection of individual privacy as possible.

Another potentially adverse consequence from anti-terrorist technology is the much wider use of microwave and other forms of radiation to which persons may be exposed. While there is no conclusive evidence at this time as to such adverse impact, it is important that such technologies be designed, perfected, and operated so as to minimize the possibility of any such effects. The more widespread use of specific antibiotics, such as Cipro, also poses potential unintended consequences. This is evidenced by a recent study which "found that a powerful strain of salmonella developed a resistance to the antibiotic Cipro in less than two years."[63]

A different kind of unintended consequence has emerged from the current effort to establish a comprehensive computer network to track foreign students in the U.S. "Officials concede they do not know . . . where [or whether] the 547,000 people holding student visas are attending school . . . [H]igher education institutions . . . raised a raft of objections [to the planned system] . . . The issue is particularly pressing for community and technical colleges, which rely heavily on foreign students because they pay higher tuition . . . [C]olleges have also objected to a plan . . . that would prevent foreign students from receiving diplomas until they confirm that they have either returned home or have extended their visas."[64] It is clear that this planned computerized, surveillance system of foreign students would pose major unintended consequences for the academic institutions involved.

Perhaps the ultimate, tragic example of the 'Law of Unintended Consequences' is the fact that without the Internet, cell phones, and modern telecommunications systems, the Al Queda network could never have evolved into the pervasive, pernicious web of evil it has become. So in that warped sense, the terrible tragedy of September 11 was—at least in some small part—an unintended consequence of the proliferation of those technologies.

The lesson from all this is that technologies often have unintended, ancillary effects which—to the extent feasible—should be anticipated and taken into account in selecting among alternative technological solutions and structuring their implementation. The point is not that any particular technology is inherently good or bad, but rather that its relative benefits and detriments depend partially on its ancillary consequences, as well as on the uses to which it is put and the way in which it is implemented.

Technology Assessment

The analysis, comparison, and selection of technologies to be implemented is a complex, difficult process. Discerning unintended consequences is not the only hurdle that must be overcome. The process involves the following components:

- determining the technical capabilities of the technology;
- evaluating its effectiveness in achieving its primary objectives;
- ascertaining its costs;
- delineating the benefits it confers;
- anticipating its ancillary consequences and estimating their positive and negative effects;
- discerning its probable impact on the economy, environment, society, and individual values;

- comparing the technology with alternatives in terms of all the foregoing factors; and
- delineating the advantages and disadvantages—the pros and cons—for the various policy options confronting decision makers.

Technology assessment is the methodology for conducting such analyses. Focused on the future, "it is the institutionalization of a methodology for previewing potential effects of technological developments so that the information generated may increase our ability to forestall the detrimental effects and encourage the beneficial effects of our inventions."[65] Incorporating elements of operations research, systems analysis, cost-benefit studies, game theory, linear programming, simulation studies, and alternative-futures scenarios—along with pragmatic public policy considerations—technology assessment emerged as a distinct field of academic research in the mid-1960s.

Prompted by information on this field from the academic and scientific communities, along with congressional concern with comprehending the technological aspects of public policy issues, Representative Emilio Q. Daddario began a public dialogue in March 1967, when he "introduced a bill proposing the creation of a 'Technology Assessment Board' . . . to provide Congress with an 'early warning signal' of the potential good and bad consequences of technological programs." As Chairman of the Subcommittee on Science, Research, and Development of the Committee on Science and Astronautics, Congressman Daddario followed up by launching several years of seminars, studies, and hearings with substantial input from reports by the Legislative Reference Service [now the Congressional Research Service] and by each of the National Academies of Science, Engineering, and Public Administration.[66]

Based on these extensive deliberations, a revised bill was introduced in the House in 1971, and followed by a companion bill in the Senate. With further amendments, the bill passed the House in February 1972; and, with some additional revisions, the bill to create an Office of Technology Assessment passed the Senate in September 1972. After consideration by a conference committee and final passage in both Houses, the Technology Assessment Act of 1972 was signed into law by President Nixon on October 13, 1972,[67] thereby establishing OTA as only the third support agency of the Congress in the history of the Republic. (The first, the Legislative Reference Service, which later became the Congressional Research Service, was created in 1914; the second, the General Accounting Office (GAO) came in 1921; and the fourth, the Congressional Budget Office (CBO), was not created until 1974.)

OTA's Unique Role and History

Under the enabling statute, OTA consists of a Technology Assessment Board (TAB) and a Director. TAB consists of 6 Senators and 6 House members, evenly split between the two parties (to ensure non-partisanship), along with the Director as an ex officio nonvoting member. The Senate members are appointed by the President pro-tempore of the Senate; the House members by the Speaker of the House; and the Director is appointed by the Board. The

Director appoints the office staff. In addition, there is a Technology Assessment Advisory Council (TAAC), whose 10 public members are appointed by the Board and which includes 2 ex officio members, the Comptroller General and the Director of the Congressional Research Service.[68]

During the 5 years of extensive consideration before this measure was enacted into law, a great deal of attention was focused on the question of why a new Office of Technology Assessment (OTA) was needed, rather than relying on the existing congressional support agencies of the General Accounting Office (GAO) and the Congressional Research Service (CRS). The overwhelming judgment of the academic, scientific, technical, and public policy communities was that neither GAO nor CRS was capable of doing the job of technology assessment required by the Congress. Indeed, "both the Comptroller General and the Director of the Congressional Research Service (and also the Librarian of Congress) support[ed] the establishment of an OTA."[69]

In the first appropriations hearings on OTA, Representative John Davis, the ranking House Democrat on the newly created Technology Assessment Board (TAB) stated: "[OTA] would perform a function far greater than could be performed by [CRS] . . . inasmuch as much of the information that would be desirable to have on the part of the committees of both the House and of the Senate would . . . require the generating of information rather than simply the retrieval of information." And the ranking House Republican on TAB, Representative Charles Mosher said: "GAO . . . investigations have been after the fact. The type of investigation they do is in retrospect . . . OTA . . . investigations are before the fact. They are . . . an early warning system for the Congress and I think that is a very important distinction . . . [Also] assessments . . . are assigned to OTA . . . by a request from congressional committees . . . The [Congressional] Research Service is responsive to any request of a Congressman and, therefore, gets a plethora of every variety, some very unimportant."[70] The issue of whether OTA's functions could be adequately performed by either CRS or GAO was re-examined in 1976 by the Commission on the Operation of the Senate, which published the conclusion that: "The functions OTA can perform represent important needs of the Senate, needs that cannot be met through the committee structure or by other support agencies."[71]

In any case, this point of view had prevailed when, a little over a year after enactment of its enabling statute, OTA received its first appropriation in November 1973, appointed its first staff in December, and commenced operations in early 1974, with then former Congressman Daddario as its first Director. Recognizing the challenge of creating a new institution within Congress, he gradually built his in-house staff, developed an extensive network of consultants and advisory panelists, and focused on establishing good working relationships with the various congressional committees. He structured OTA's initial assessments into seven program areas: energy, food, health, materials, national R&D policies and priorities, technology and international trade, and transportation.

After guiding OTA through its formative first four years, he resigned in 1977, and was succeeded in 1978 by the former governor of Delaware, Russell Peterson. Unlike Daddario, Peterson did not manage to develop good relationships with the TAB Members who had appointed him. "Several members of the board felt that . . . [his] priorities . . . strayed too far from what Congress considered to be the most important legislative concerns . . . One [TAB Member] complained that Peterson was trying to create a 'sort of Brookings Institution in the Congress' . . . another accused the OTA of a 'disturbing pattern of ignoring congressional oversight and service'."[72] In any event, Peterson resigned in 1979 after serving only one year as Director.

OTA achieved maturity with its next Director, Dr. John Gibbons who served close to 15 years, from 1979 to 1993. He developed very good relationships with TAB Members and congressional committees and, through astute management of OTA, built the Office's credibility within the Congress and throughout the nation's academic, scientific, technical, and professional communities. Indeed, OTA "gradually became recognized worldwide as the top institution of its kind . . . Austria, Denmark, the European Community, France, Germany, Great Britain, the Netherlands, and Sweden have copied or adapted the OTA style. Similar organizations are being discussed or formed in Hungary, Japan, Mexico, the People's Republic of China, Russia, Switzerland, and Taiwan."[73]

From 1974 through 1995, "OTA published nearly 750 full assessments, background papers, technical memoranda, case studies, and workshop proceedings. The quality of those products is attested to by the facts that from 1992 to 1994, twelve assessments won the National Association for Government Communicators' prestigious Blue Pencil Award . . . [and during] the same 3 years, 12 additional reports were named among the 60 Notable Government Documents selected annually by the American Library Association's Government Documents Roundtable—representing the best Federal, State, and local government documents from around the world . . . OTA's reports were often bestsellers at the Government Printing Office and the National Technical Information Service . . . [For example,] GPO sold 48,000 OTA reports in [one year] alone."[74]

The authoritative credibility achieved by OTA over the years is perhaps best articulated in a 1988 article entitled "Influential Office Guides Congress into Space Age," in which the author asserts: "Without OTA's nod, leading scientific theories stand little chance of winning status as conventional wisdom on Capitol Hill . . . The Office is credited with having matured into the scientific heavyweight whose assessments can mean life or death for technical problems in the appropriations process . . . At least one thing is clear: in a town where unimpeachable sources are oh-so-hard to come by, OTA has managed to secure a position near the top of the list."[75]

OTA's Structure and Pattern of Operations

OTA achieved this status as a consequence of the prescience embodied in its enabling statute and the implementing pattern of operations that subsequently evolved. Although the bill that originally passed the House called for the majority party to hold a majority of seats on TAB, the Senate bill stipulated a board evenly divided between the two parties, and the Senate version was accepted in conference.[76] This assurance of TAB's non-partisanship—highly unusual at a time when both Houses of Congress had been controlled by the Democrats for a generation—was absolutely essential for enabling OTA to realize both the reality and public perception of objectivity and credibility.

Along with a governing board, evenly split between House and Senate and between Democrats and Republicans, the Act called for the creation of an advisory council, including: "ten members from the public . . . eminent in one or more fields of the physical, biological, or social sciences or engineering or experienced in the administration of technological activities, or . . . qualified on the basis of contributions made to educational or public activities."[77] Thus the Act provided TAB and the Director with the perspective of an eminent group of outside advisers. Since the assessments to be undertaken by OTA, however, spanned a multitude of scientific and technical disciplines and specialities, OTA also built a network of advisory panels and consultants who were versed in the specific issues involved in particular assessment projects. Over the years as the OTA in-house staff grew to number nearly 150, this outside network of advisers grew to about 1,000 individuals throughout the nation.

The professional staff consisted of about half scientists and engineers and about half social scientists, lawyers, and health care professionals. From 1979 on, the OTA staff was organized in three divisions, each headed by an Assistant Director of OTA. These were the divisions of: (a) Energy, Materials, and International Security; (b) Science, Information, and Natural Resources; and (c) Health and Life Sciences. Each division in turn was organized in three programs, headed by a Program Director. The programs in division (a) were: Energy and Materials; Industry, Technology, and Employment; and International Security and Commerce. The programs in division (b) were: Communications and Information Technologies; Oceans and Environment; and Science, Education, and Transportation. And the programs in division (c) were: Biological Applications; Food and Renewable Resources; and Health.

Each program in turn usually had several projects underway at any one time, each of which was headed by a project director. Some relevant examples of specific OTA assessments include:

- *The Border War on Drugs*
- *Electronic Surveillance in a Digital Age*
- *High Level Radioactive Waste Site Characterization*
- *Impacts of Antibiotic-Resistant Bacteria*
- *New Developments in Biotechnology*
- *Scientific Validity of Polygraph Testing*
- *Taggants in Explosives*
- *Technology Transfer to China*
- *Technology and Counter Terrorism*
- *Transportation of Hazardous Materials*
- *Virtual Reality and Technologies for Combat Simulation*
- *Technologies Underlying Weapons of Mass Destruction*

As noted above, in addition to the in-house staff and the congressional board and advisory council, OTA made extensive use of a national network of about 1,000 advisory panelists and consultants who addressed specific assessment projects. Thus for each full-fledged assessment an advisory panel of about 12–20 individuals was appointed which included scientific and technical experts in the particular subject under consideration, as well as participants from industry, labor, academia, the professions, state and local government, and the public at large. And before an assessment report was finalized, it was critiqued by a wider array of experts and stakeholders throughout the nation.[78]

"The steps in the assessment process may be summarized as follows: (1) OTA staff engage in informal communication with congressional committee staff. (2) This leads to formal committee request letters to OTA, a proposal from the staff to TAB, and TAB approval to initiate an assessment. (3) An advisory panel is appointed which critiques the staff's preliminary assessment design at the panel's first meeting. (4) Months later, at the second panel meeting, OTA discusses its analysis of the data it has obtained and the way it is likely to be handled in the assessment report. (5) Some months later OTA presents a draft of its final report to the advisory panel and subsequently to additional outside reviewers. (6) About eighteen months after the start of the project, OTA presents a final report to TAB for approval to release it to the requesting committees and the public at large. (7) OTA then presents its results to the requesting committees, in the form of briefings and testimony at hearings, as well as in a written document, and disseminates its findings to appropriate Executive Branch agencies, other interested parties, and the general public." [79]

OTA's Credibility, Objectivity, and Relevance

While this process may appear lengthy and laborious, it embodies an elaborate panoply of checks and balances that confer credibility, objectivity, and relevance on the final assessment report. These checks and balances are inherent in OTA's statute and pattern of operations. Some of the most important ones are:

- the even balance between House and Senate and the two parties on TAB;
- the tradition of choosing the Vice Chair from the opposite party to the Chair;
- the need for TAB approval both to initiate an assessment and subsequently to release the final report;
- the Technology Assessment Advisory Council's salutary influence on OTA's standards of excellence;
- each advisory panel's role in the design of the assessment, the analysis of the data, and the content of the final report;
- the role of the stakeholders and additional expert consultants in reviewing the draft report;
- the presentation of a Review Memorandum from the Project Director to the OTA Director, which "describes the reactions of the panel and outside reviewers to each portion of the report and shows how the final version takes account of those comments;" [80] and

- the pattern of continuing, informal communication between OTA and committee staff before, during, and as follow-up to the assessment.

The relevance of OTA's assessments is ensured by the close control the congressional board exercises over the initiation and final approval of OTA products, as well as by the continuing communication between OTA and congressional committee staff. While OTA reports have received widespread acclaim throughout the academic, scientific, technical, and professional communities, their primary purpose is not to edify scholars, but rather to serve congressional needs for the analysis of policy options involving technology. Because of the continuing oversight of TAB and interaction with congressional committees, adherence to this purpose is preserved.

OTA's objectivity is ensured through a number of the checks and balances, the most fundamental one of which is that the Board is evenly split between the two parties and has traditionally included a range of conservatives, moderates, and liberals among its members. Moreover, the pattern of choosing the Chair and Vice Chair of TAB from opposite parties adds to OTA's non-partisanship, and hence its objectivity. This characteristic is further enhanced by the roles played by the advisory council, the specialized advisory panels, and the many outside reviewers involved in each assessment. They comprise not only a very wide range of technical experts, but stakeholders as well—representatives of industry, labor, public interest groups, and the public at large.

This diversity of expertise and points of view ensures that the OTA staff is aware of virtually all relevant issues and interests involved in the particular assessment. The fact that the final Review Memorandum has to show specifically how each concern has been taken into account accords a high degree of objectivity to the final OTA report. Attesting to that objectivity is the fact that in debates on congressional proposals, OTA reports were oftentimes cited by both the proponents and opponents of the particular proposal. OTA's credibility consequently comes from the entire assessment process and the enviable reputation OTA achieved during the Gibbons directorship.

The Relative Roles of OTA, CRS, and GAO

Having this understanding of the OTA process, it becomes clear that Congress made the right decision in establishing OTA in 1972, rather than attempting to rely on CRS and GAO for providing the necessary analysis of policy options involving complex technological issues. Congress needs technology assessment that is timely, targeted to the specific legislative priorities of congressional committees, and presented in a format that clarifies the consequences—both pro and con—of the various policy options related to the technologies under consideration.

Neither CRS nor GAO has the capability to design and conduct such assessments. Both CRS and GAO must respond to the requests of individual members of Congress; whereas OTA responds only to requests from congressional committees. Accordingly, OTA assessments are inherently oriented toward the priority needs of congressional committees, thereby rendering them relevant to the committees' legislative agendas. This legislative relevance is further ensured by the requirement for TAB approvals both to initiate assessments and release final reports, as well as its continuing oversight of OTA activities throughout the process. While CRS research and GAO investigations certainly provide valuable information to individual members of the Senate and the House, they cannot possibly attain the same degree of conformance to committees' legislative requirements.

Furthermore, as former Representative Davis noted, CRS essentially retrieves existent information, while OTA generates new information. And as former Representative Mosher stated: GAO does retrospective investigations; whereas OTA assessments are future oriented and serve as "an early warning system for the Congress . . . a very important distinction."[81]

Finally, neither CRS nor GAO has the statutory authority or institutional capability to make as extensive use of outside advisers drawn from all segments of the scientific, technical, professional, and public interest communities as OTA has. As indicated earlier, these advisers have played an integral, essential role in ensuring that OTA reports take account of virtually all relevant expertise and points of view. Without that involvement, OTA's products could not have been able to achieve so high a level of objectivity and credibility as they did. Neither CRS nor GAO is equipped to make that kind of use of 1,000 consultants.

When one considers that OTA is controlled by a congressional board—similar to a joint committee—and has maintained continuing communication with congressional committees, along with the pattern whereby the office has drawn upon its pool of about 1,000 outside advisers, the essence of OTA's unique role becomes clear. In effect, OTA has served as a critical translation link between the widespread technical knowledge of the academic, scientific, and professional experts and the policy-oriented queries and concerns of congressional committees. OTA effects this translation in a thorough, in-depth fashion that focuses on future-oriented policy options for Congress. In brief, OTA is the interface between Congress and the nation's science and technology community. For all of the reasons that have been cited, neither CRS nor GAO can fulfill that function.

OTA After Gibbons: 1993–1995

After 15 years of high achievement as OTA Director, Gibbons resigned in early 1993 to join the new administration as Science and Technology Adviser to the President and Director of the White House Office of Science and Technology Policy. He was succeeded by Dr. Roger C. Herdman who had been serving as an OTA assistant director, with responsibility for the Health and Life Sciences Division. In his new role, Dr. Herdman carried on in the tradition of excellence established by his predecessor.

However, in 1995 there was a sea change in control of Congress. The new leadership was intent on eliminating a number of cabinet departments—Energy, Education, and Commerce—and also on reducing the costs of government, including within the Legislative Branch. The likeliest target for reduction within the Congress was one of the support agencies, CBO, CRS, GAO, and OTA. Of these, OTA was the smallest and most vulnerable.

Accordingly, in order to save money—the FY 1995 appropriation for OTA had been $22 million—the House Appropriations Committee on June 15, 1995 recommended elimination of funding for OTA. On June 22 following a failed effort by Representative Vic Fazio (D-CA) to restore OTA funding, the House passed the FY 1996 Legislative Branch Appropriations bill with no funding for OTA. The House also eliminated the Joint Committee on Printing, reduced the Joint Economic Committee budget by 25 percent, cut House committee budgets overall by a total of $40 million, and the GAO budget by $57 million. So the elimination of OTA's appropriation occurred within a context of extreme cost-cutting measures across the board. [82]

On July 18 the Senate Appropriations Committee reported out its bill, including $3.6 million for OTA—but solely for the purpose of closing down the office. Senator Ernest F. Hollings, who had served on the OTA board for 23 years, had led an unsuccessful fight in committee to restore full funding. Again on the Senate floor on July 20, he offered an amendment to the committee bill to provide OTA with $15 million. Although his amendment was supported by then Minority Leader Daschle, Appropriations Committee ranking Democrat, Senator Byrd, as well as all other senators who had served on the OTA Board—Senators Grassley, Hatch, Kennedy, and Stevens—it still went down to defeat.

"While lauding the past successes of the Office of Technology Assessment (OTA), [opponents of the amendment] stated that Senators . . . should support efforts to conserve taxpayers' funds and streamline the bureaucracy surrounding Congress." [83] Senator Hollings retorted: "What you're doing is eliminating the most economical approach to this technological need." [84] Senator Kennedy said: "The Office of Technology Assessment . . . continues to serve an indispensable role . . . it should not be abolished." Senator Grassley noted: "OTA is our source of objective counsel when it comes to science and technology and its interaction with public policy decision making . . . [I]f we do not have an unbiased source of information, then we have to rely on organizations with a stake in keeping alive programs that benefit their interests." Senator Hatch added: "OTA . . . is the one arm of Congress that does give us ... unbiased, scientific and technical expertise that we could not otherwise get where most everybody has confidence in what they do." And Senator Stevens stated: "[W]e are about ready to do away with the one entity in the Congress that tries to . . . deliver to Members of Congress credible, timely reports on the development of technology. I believe . . . that we are changing the course of history in this Congress, but this is not one of the hallmarks of that change. This entity (OTA) ought to be out in the forefront of that change, and it will not be unless it is properly funded and maintained." [85]

In the conference committee, Representative Fazio made another unsuccessful attempt to restore funding for OTA. In that debate Representative Ray Thornton (D-AK) made a rhetorical connection between the elimination of OTA's funds and the inclusion in the bill of funds to renovate the congressional Botanic Garden. He said: "The arguments that there are alternatives to OTA apply equally to [the Botanic Garden, which] could be privatized. There are florists all over the country. If we're going to cancel the garden of the mind—OTA—then we can't afford to keep a [Botanic] garden."[86]

The House adopted the conference report on September 6, and the Senate followed suit on September 22, with a proponent of the bill stating: "This bill sets the standard. If we in Congress can cut our own budget, every federal agency should be able to do the same." The President vetoed the bill on October 3, because Congress submitted it to him prior to passing appropriations measures for various Executive Branch departments and agencies. After reintroducing the identical bill, the House passed it again on October 31, and the Senate on November 2. This time the bill was sent to the President, coupled with the appropriation for the Treasury Department and the White House, and he signed it into law on November 17.[87] OTA had already ceased regular operations on September 29, the last work day of FY 1995. A skeleton staff was retained for a few months at the start of FY 1996, in order to archive OTA's records, arrange for internet access to its reports at various university sites, close out its personnel and financial commitments, dispose of its computers, furniture, and other equipment, and prepare its Annual Report to Congress for FY 1995.[88]

* * * * *

Findings

The findings that emerge from the foregoing discussion are as follows:

- Technology is critical to U.S. success in the War on Terrorism and ensuring homeland security.
- A wide variety of sophisticated technologies may be involved in those efforts.
- Choosing among possible technologies and patterns of implementation is a complex process, oftentimes involving unintended consequences.
- Technology assessment is the methodology for making such choices.
- The leading exemplar of technology assessment was the congressional Office of Technology Assessment (OTA).
- For almost a quarter of a century, OTA provided Congress with valuable analyses of policy options on important issues involving technology.
- During that period OTA achieved a world-wide reputation for excellence, as a non-partisan, objective, and credible conductor of technology assessments.
- There was no dissatisfaction with its performance; indeed OTA received accolades for its excellent work while its funding was being eliminated.
- Elimination of its funding was a cost-cutting measure at a time of fiscal stringency and a symbol for Executive Branch agencies to emulate.

- Congress now needs its own source of non-partisan, objective technology assessment in order to fulfill its legislative, appropriation, and oversight responsibilities in the War on Terrorism and ensuring homeland security.

CONCLUSION

Fortunately, in 1995 when OTA's funding was discontinued, its enabling statute remained in effect; no action was taken to rescind it. So the law establishing OTA is still on the books. OTA still technically exists. For practical purposes, what does this mean?

To determine its import, it's necessary to examine the provisions of the enabling statute, the Technology Assessment Act of 1972. Section 3(b) of the act states that OTA "shall consist of a Technology Assessment Board . . . and a Director." Discontinuing OTA's funding vacated the positions of the director and the staff, but the Board still technically exists. Moreover, since the Senate is a continuing body and the act does not limit the tenure of its members, the Senators who were Board members in 1995—Senators Grassley, Hatch, Hollings, and Kennedy—are still Board members. Since the House is not a continuing body, it could be argued that the current House members who were on TAB in 1995—Representatives Dingell, Houghton, McDermott, and Oxley—would not still be members. However, the facts that TAB is an independent board, rather than a congressional joint committee and that the OTA statute does not impose any time limit on board appointments provide a basis for arguing that they still are members of TAB. In any case, section 4(b) of the act stipulates that: "Vacancies in the membership of the Board shall not affect the power of the remaining members to execute the functions of the Board." In addition, the appropriations section of the act, section 12(a) states that: "To enable the Office to carry out its powers and duties, there is hereby authorized to be appropriated to the Office [following its first 2 fiscal years of existence] . . . "thereafter such sums as may be necessary."[89]

In short, OTA has an ongoing authorization to receive appropriations, and the Technology Assessment Board (TAB) is empowered to submit a recommendation to the Appropriations Committee for such an appropriation. Given these facts and the finding that Congress needs its own source of technology assessment to fulfill its role in the War on Terrorism and ensuring homeland security, it is the conclusion of this author that OTA should be reactivated.

But to underscore the urgent necessity for reactivating OTA, it is instructive to consider one final example of OTA's potential impact on the War on Terrorism and homeland security. As is well known, the anthrax attacks last fall engendered considerable confusion and consternation among public health authorities, public safety officials, and policy makers throughout federal, state, and local government. There was great uncertainty as to the source and extent of the attacks, the potency and persistence of the anthrax spores, the manner of transmission, and—not least—the number of spores necessary to trigger inhalation anthrax in human beings. In the course of reacting to the attacks, it was widely reported that it was believed that 8,000–10,000 spores would have to be inhaled for a person to contract inhalation or pulmonary anthrax. This belief undoubtedly played a role in shaping the public health response to the attacks.

It's unfortunate that OTA was not operational at that time. If it had been, OTA staff could have ensured that a 1993 OTA report was promptly brought to the attention of the public health authorities. The report entitled *Technologies Underlying Weapons of Mass Destruction* contained the following finding: "1,000 spores or less can produce fatal pulmonary anthrax in some members of an exposed population."[90] If this information had been readily available, it's conceivable that it even could have saved a life or—at the very least—afforded much better guidance to the public health authorities in designing their response to the crisis.

* * * * *

RECOMMENDATIONS

The War on Terrorism and the striving for homeland security are urgent national necessities. However, the reactivation of OTA is equally urgent, if Congress is to be empowered to partner with the President in pursuit of those objectives—in its role as a co-equal branch of government.

The sooner Congress can reactivate OTA, the sooner it can effectively deal with those issues. Once OTA receives an appropriation, it still will take some months to build its staff and network of outside advisers, and to work with the congressional committees to delineate an assessment agenda that meets their priority needs. At this time of national challenge, waiting until the start of the next fiscal year, October 1, 2002, is too long a period to remain without this resource. Accordingly, an appropriation for OTA should be included in the next supplemental appropriations bill to come before the Congress.

A key question then becomes: How much should be provided for OTA in this bill? In the current situation of fiscal stringency, one should allocate only enough to reactivate the office effectively. This in turn hinges on what the office would be doing for the balance of this fiscal year.

After a few essential staff members have been appointed, their primary function would be to canvass and consult with congressional committees in both the House and Senate in order to ascertain their priority needs for technology assessments with respect to the War on Terrorism and homeland security. The task would then be to plan a series of assessments designed to meet those priority needs. Concurrently with these activities, the office would be identifying potential outside advisers on whom OTA could rely, and under the guidance of the Technology Assessment Board, preparing a detailed budget submission for the following fiscal year that would provide OTA with the resources to proceed with a number of high priority assessments.

It is believed that a supplemental appropriation of $1 million would be sufficient for OTA to carry out these initial activities effectively. Considering that this $1 million would reactivate an Office that could aid Congress in evaluating the $38 billion the President has recently requested for homeland security, the $1 million amount does not seem unreasonable.

Recommendation: In the first supplemental appropriation bill considered in this session, Congress should include $1 million for OTA to canvass and consult with congressional committees, and plan a series of technology assessments designed to meet the priority needs of those committees with respect to the War on Terrorism and homeland security.

* * * * *

NOTES

1. Sean Ford, "Small Influential Office Guides Congress Into Space Age," *Federal Times*, 13 June 1988, 18.

2. U.S. Congress, Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction,* December 1993, 78.

3. William J. Broad, Stephen Engelberg, and James Glanz, "A Nation Challenged: The Threats; Assessing Risks, Chemical, Biological, Even Nuclear," *New York Times*, 1 Nov. 2001, AI.

4. John Schwartz, "A Nation Challenged: The Computer Networks; Cyberspace Seen as Potential Battleground," *New York Times*, 23 Nov. 2001, B5.

5. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998) 180–181.

6. It should be noted that water systems are vulnerable not only to chemical or biological contamination, but also to cyber-terrorism: ". . . essentially every component of the water supply system is highly automated. This includes electronic control of water pumping and storing, water treatment operations, and water transmission . . . [G]reat damage could be done if the control of these systems were lost for a period of time due to cyber attack." U.S. Congress, House Committee on Science. "Safety of Our Nation's Water," testimony by Richard G. Luthy, Professor of Civil and Environmental Engineering, Stanford University and Chair, Water Science and Technology Board, National Research Council, 107th Cong., 1st sess., 14 Nov. 2001.

7. Matthew L. Wald, "Electric Power System Is Called 'Vulnerable,' and Vigilance Is Sought," *New York Times*, 28 Feb. 2002, A11.

8. President George W. Bush, "State of the Union," U.S. Capitol, Washington, D.C., 29 Jan. 2002.

9. *Ibid.*

10. Phillip B. Heymann, *Terrorism and America: A Common Sense Strategy for a Democratic Society* (Cambridge: The MIT Press, 1998) 134–136.

11. Mary Jordan, "Ridge Calls Security at Border 'Outdated'," *Washington Post*, 6 March 2002, A11.

12. Robert Montgomery, "A Look at Cellular's Alarming Technology," *Mastering Security* (Dubuque: Kendall/Hunt, 1996) 12.

13. Robert De Lia, "Seeing Into the World of Fiber Optics for Security," *Mastering Security* (Dubuque: Kendall/Hunt, 1996) 17.

14. Donald R. Jones, Jr., Executive Vice President, NetTalon Security Systems, Inc., Personal Interview, 6 Dec. 2001.

15. U.S. Congress, House Committee on Science. "Aviation Security: Technology's Role in Addressing Vulnerabilities," testimony by Keith O. Fultz, Assistant Comptroller General, Resources, Community, and Economic Development Division, General Accounting Office, 19 Sept. 1996, 7–12.

16. National Research Council, *Detection of Explosives for Commercial Aviation Security,* Executive Summary (Washington, D.C.: National Academy Press, 1993), 7–12.

17. Jim Dawson, "National Labs Focus on Tools Against Terrorism in Wake of Airliner and Anthrax Attacks," *Physics Today*, Jan. 2002, 19–22.

18. U.S. Congress, House Committee on Science. "Aviation Security," 8–9.

19. Cynthia L. Webb, "A Handy Security Solution: Aether Software Gets Tryout on Handhelds at Boston Airport," *Washington Post*, 16 Jan. 2002, E5.

20. National Research Council, *Airline Passenger Security Screening: New Technologies and Implementation Issues,* Executive Summary (Washington, D.C.: National Academy Press, 1996) 3.

21. Jeffrey Rosen, "A Watchful State," *New York Times*, 7 Oct. 2001, 6–38.

22. Donald R. Richards, "ID Technology Faces the Future," *Mastering Security* (Dubuque: Kendall/Hunt, 1996) 78.

23. U.S. Congress, House Committee on Science, "Cyber Security: Beyond the Maginot Line," testimony by Wm. A. Wulf, President, National Academy of Engineering and AT&T Professor of Engineering and Applied Science, University of Virginia, 107th Cong., 1st sess., 10 Oct. 2001.

24. Robert O'Harrow Jr., "Key U.S. Computer Systems Called Vulnerable to Attack; Defense, FAA Among Agencies Lacking Security, Experts Say," *Washington Post*, 27 Sept. 2001, A6.

25. Sada Yoshi Ohbu, et al., "Sarin Poisoning on Tokyo Subway," *Southern Medical Journal,* 3 June 1997, 1.

26. Lyndsey Layton, "Drill Tests Response to Attack In Metro; Exercise Gauges Chemical Threats," *Washington Post*, 5 Dec. 2001, B8.

27. Dawson, "National Labs Focus," 19–20.

28. Ellen Nakashima, “USPS Sees New Way to Spot Biohazards,” *Washington Post*, 9 Mar. 2002, A13.

29. Marian Burros, “Eating Well; A Vulnerable Food Supply, A Call for More Safety,” *New York Times*, 31 Oct. 2001, Fl.

30. National Research Council, *Improving Civilian Medical Response to Chemical or Biological Terrorist Incidents,* Executive Summary (Washington, D.C.: National Academy Press, 1998) 3.

31. Ceci Connolly, “Bush Promotes Plans To Fight Bioterrorism,” *Washington Post*, 6 Feb. 2002, A3+.

32. Avram Goldstein, “Anti-Terror Campaign Turns to Doctors; Physicians Scramble to Learn About Bio-Weapons; Some Urge Mandated Training,” *Washington Post*, 14 Oct. 2001, A12.

33. Joby Warrick and Steve Fainaru, “Bioterrorism Preparations Lacking at Lowest Levels; Despite Warnings and Funds, Local Defenses Come Up Short,” *Washington Post*, 22 Oct. 2001, A7.

34. National Research Council, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response,* Executive Summary (Washington, D.C.: National Academy Press, 1999) 5–6.

35. Eric Pianin and Bill Miller, “Security Permeates Budget: Many Agencies Would Share $37.7 Billion in New Funds,” *Washington Post*, 5 Feb. 2002, A7.

36. Sheryl Gay Stolberg, “A Nation Challenged: The Disease; Ill Postal Worker Has Symptoms That Stop Short of Anthrax,” *New York Times*, 11 Jan. 2002, A11.

37. David Brown, “Agency With Most Need Didn’t Get Anthrax Data,” *Washington Post*, 11 Feb. 2002, A3.

38. Dawson, “National Labs Focus,” 21.

39. Jones, Personal Interview.

40. George Musser, “Better Killing Through Chemistry: Buying Chemical Weapons Material Through the Mail is Quick and Easy,” *Scientific American*, Dec. 2001, 20–21.

41. Terence Chea, “Firm’s Anti-Nerve Gas Device Approved,” *Washington Post*, 30 Jan. 2002, E5.

42. Dawson, “National Labs Focus,” 20.

43. *Ibid.* 21.

44. John Mesenbrink, “Fighting the War on Bioterrorism,” *Security Magazine*, 4 Jan. 2002, 3.

45. Gina Kolata, “Treatments; On Many Fronts, Experts Plan for the Unthinkable: Biowarfare,” *New York Times*, 23 Oct. 2001, F4.

46. Steve Twomey, “A Recipe for Safe Mail,” *Washington Post*, 30 Jan. 2002, Al+.

47. National Research Council, *Chemical and Biological Terrorism,* 8.

48. Pianin, “Security Permeates Budget.”

49. “Freon,” *Encyclopaedia Britannica,* vol. 9, 1973 ed., 924.

50. John Schwartz, “The Irradiation of Mail Can Also Zap the Contents,” *New York Times*, 11 Feb. 2002, C2.

51. Twomey, “A Recipe For Safe Mail.”

52. Andrew DeMillo and Allan Lengel, “Fumes From Mail Sicken 11 at Commerce,” *Washington Post*, 11 Jan. 2002, B9.

53. Spencer S. Hsu, “73 Senate Workers Report Illness,” *Washington Post*, 7 Feb. 2002, B1+.

54. Spencer S. Hsu, “Workers Handling Government Mail Report Illness,” *Washington Post*, 9 Feb. 2002, A6.

55. Hsu, “73 Senate Workers Report Illness.”

56. Schwartz, “The Irradiation of Mail.”

57. Sherry L. Harowitz, “More Than Meets the Eye,” *Mastering Security* (Dubuque: Kendal1/Hunt, 1996) 73.

58. Richards, “ID Technology Faces the Future,” 79.

59. Sara Kehaulani Goo, “Nonlethal Weapons Pose Own Risks in Air, Report Says,” *Washington Post*, 6 March 2002, A11.

60. National Research Council, *Airline Passenger Security Screening,* 3.

61. Rosen, “A Watchful State.”

62. Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of the CCTV* (New York: Berg, 1999) 42.

63. AP, “Resistance Builds to Cipro, Study Says,” *New York Times*, 7 Feb. 2002, A18.

64. Kate Zernike and Christopher Drew, “Efforts to Track Foreign Students Are Said to Lag,” *New York Times*, 28 Jan. 2002, Al +.

65. U.S. Congress, Senate, *Office of Technology Assessment for the Congress,* Hearing Before the Subcommittee on Computer Services of the Committee on Rules and Administration, 92nd Cong., 2nd Sess., 2 March 1972, 72.

66. Vary T. Coates, *Technology and Public Policy: The Process of Technology Assessment in the Federal Government* (Washington, D.C., Program of Policy Studies in Science and Technology, The George Washington University) July 1972, I:14–36.

67. U.S. Congress, House, *Office of Technology Assessment: Background and Status,* Report to the Committee on Science and Astronautics, 93rd Cong., 1st Sess., Aug. 1973, 14–17.

68. "Technology Assessment Act of 1972," Public Law 92–484 (2 U.S.C 471–481).

69. U.S. Congress, Senate, *Technology Assessment for the Congress,* Staff Study of the Subcommittee on Computer Services of the Committee on Rules and Administration, 92nd Cong., 2nd Sess., 1 Nov. 1972, 41.

70. U.S. Congress, Senate, *Office of Technology Assessment,* Excerpt of Hearings Before a Subcommittee of the Committee on Appropriations, Fiscal Years 1973 and 1974, 93rd Cong., 1st Sess., 9 May & 20 June 1973, 11–14.

71. U.S. Congress, Senate, *Congressional Support Agencies,* Prepared for the Commission on the Operation of the Senate, 94th Cong., 2nd Sess., 55.

72. David Dickson, *The New Politics of Science* (Chicago: University of Chicago Press, 1998) 242.

73. U.S. Congress, Office of Technology Assessment, *Annual Report to Congress,* Fiscal Year 1995, 6.

74. *Ibid.* 7–8.

75. Ford, "Small Influential Office Guides Congress Into Space Age," 18.

76. Congressional Research Service, Library of Congress, *Office of Technology Assessment: Background and Status,* Aug. 1973, 13–17.

77. "Technology Assessment Act," sec. 7(a).

78. U.S. Congress, Office of Technology Assessment, *What OTA Is—What QTA Does—How OTA Works,* 1989, 8.

79. Mottur, Alfred E., *Institutional Innovation in the Congress: The Office of Technology Assessment (OTA),* "Sentinels of the Republic Scholar" Honors Thesis, Williams College, Williamstown, MA, 1989, 37.

80. *Ibid.* 108.

81. U.S. Congress, Senate, *Office of Technology Assessment,* Excerpt of Hearings, 1973, 11–14.

82. *CQ Almanac*, "Congress Cuts Legislative Funds," 1995, 11–61.

83. U.S. Congress, Senate Democratic Policy Committee, Senate Voting Record, No. 316, "Legislative Branch Appropriations, 1996, OTA," July 20, 1995.

84. *CQ Almanac*, 11–64

85. U.S. Congress, Office of Technology Assessment, *Annual Report,* 36–38.

86. CQ Almanac, 11—64–65.

87. *Ibid.* 11–65.

88. U.S. Congress, Office of Technology Assessment, *Annual Report,* 40.

89. "Technology Assessment Act," sec. 3(b), sec. 4(b), and sec. 12(a).

90. Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction,* 78.