TECHNOLOGY AGAINST TERRORISM

THE FEDERAL EFFORT

Summary

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT

Office of Technology Assessment

Congressional Board of the 102d Congress

TECHNOLOGY AGAINST TERRORISM

THE FEDERAL EFFORT

Summary

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT

Foreword

The United States has been a prime target of international terrorism for at least two decades. In the 1980s, several terrorist attacks had a particularly powerful effect in mobilizing public opinion and government action. These were the bombings of the U.S. Embassy and of the U.S. Marine Barracks in Beirut in 1983, and the destruction of Pan American Flight 103 over Lockerbie, Scotland in 1989. The Federal Government reacted in both cases by devoting more attention and resources to developing strategies and tools to defend U.S. lives and interests against such outrages. Unless underlying causes are eliminated, terrorist attacks will continue. Since they may change in type and scope, the United States must be prepared to deal with a wide range of eventualities. The widespread availability of sophisticated weapons makes the challenge of counterterrorism all the more difficult.

In 1989, the Senate Committee on Governmental Affairs; the Senate Subcommittee on Terrorism, Narcotics, and International Operations of the Senate Committee on Foreign Relations; and the Senate Committee on Commerce, Science, and Transportation, together with its Subcommittee on Aviation, requested the Office of Technology Assessment to investigate the status of research on technological means to protect ourselves against terrorist threats. A later endorsement of the study was received from the Senate Select Committee on Intelligence.

This report is the first of two in response to these requests. A classified version was transmitted to Congress on September 24, 1990. It deals with the Federal research and development effort in countering terrorism, and with the state of attempts to use technology to aid in detecting and preventing attempts to introduce explosives aboard aircraft. A review of the relevant R&D programs in many agencies is provided. The second report of this study will be released in summer 1991.

The help and cooperation of many scientists and officials from the Departments of Defense, Energy, Justice, State, Transportation, and Treasury, and the Intelligence Community are gratefully acknowledged.

John H Gibbons

JOHN H. GIBBONS
Director

The Use of Technology in Countering Terrorism Advisory Panel

Marvin Goldberger, *Chair*
Director, Institute for Advanced Study
Princeton, New Jersey

Peter F. Bahnsen
Executive Vice President
MLI International, Ltd.

Terry Bearce
Program Manager on Low Intensity Conflict
Los Alamos National Laboratory

Homer Boynton
Managing Director for Security
American Airlines

L. Paul Bremer
Managing Director
Kissinger Associates

Chris Chicles
C.H. Chicles & Associates

Arthur Donahue
President
Softworld Marketing, Inc.

Lee Grodzins
Department of Physics
Massachusetts Institute of Technology

Chris Hatcher
Department of Psychiatry
University of California, San Francisco

Carolyn Imamura
Pacific Basin Development Council

Wilfred A. Jackson
Airport Operators Council International

Jim Jacobs
Director, Nuclear Security Systems
Sandia National Laboratory

Brian Jenkins
Managing Director
Kroll Associates

Michael K. Johns
President
Johns & Bhatia Engineering Consultants, Ltd.

Donald Kerr
President
EG&G, Inc.

Joseph Krofcheck
President
Yarrow Associates

Robert Kupperman
Senior Advisor
Center for Strategic and International Studies

Richard Porter
Aerospace Services International, Inc.

Billie H. Vincent
Aerospace Services International, Inc.

Stanley Wiener
Professor of Internal Medicine
University of Illinois, Chicago

Joshua Lederberg (*ex officio*)
Rockefeller University
Vice Chairman,
Technology Assessment Advisory Council

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the advisory panel members. The panel does not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

The Use of Technology in Countering Terrorism
OTA Project Staff

Lionel S. Johns, *Assistant Director, OTA*
Energy, Materials, and International Security Division

Alan Shaw, *International Security and Commerce Program Manager*

Anthony Fainberg, *Project Director*

Michael B. Callaham

Kevin Dopart[1]

Deborah L. Kyle[2]

Russell L. Maxwell[3]

Edith Page[4]

Peter H. Rose[5]

Administrative Staff

Jackie Boykin

Louise Staley

Donna Reynolds

Contractor

Yonah Alexander

[1]On assignment from OTA's Science, Education, and Transportation Program.
[2]Department of Commerce Science and Technology Fellow, 1989-90.
[3]On assignment from Sandia National Laboratories.
[4]On assignment from OTA's Science, Education, and Transportation Program.
[5]AAAS Fellow, 1989-90

INTRODUCTION

The United States has been a favored target of terrorists for well over a decade. During much of this time, public and governmental reaction to terrorist atrocities committed against U.S. civilians, military and diplomatic personnel, or property—at home or abroad—tended to be short-lived. Typically, an event produced a short period of anger and outrage lasting a few days, or, perhaps, weeks. There were occasional calls for Federal action but little of substance was accomplished. Interest would slowly abate until the next major incident reinitiated the sequence. Recently, however, the U.S. response, in attitude and action, has begun to show some staying power.

The 1983 Beirut attacks on the U.S. Embassy and Marine barracks, killing 258 Americans, constituted one watershed. Following these incidents, two investigative commissions were formed: one, within the Department of Defense and chaired by Admiral Robert L.J. Long, was assigned the task of investigating the bombing of the barracks; the other, chaired by former CIA Director Bobby Inman, investigated measures to improve security at U.S. embassies and consulates abroad. The Long Commission recommended, among other things, a change in national policy that would incorporate a more proactive approach in dealing with terrorism. The main thrust of the report, however, was to elevate the importance of dealing with terrorism to a national priority. The Commission considered terrorism to be a form of warfare and to require appropriate responses. Among these responses would be a higher profile for those activities within Federal agencies that were designed to protect against or to fight terrorism. Recommendations of the Inman Commission included a massive improvement of security at State Department facilities overseas, including: personnel protection, building security improvements, and design and structural changes. Also, the post of Ambassador-at-Large for Counterterrorism was created. A major diplomatic security program was initiated and continues today.

Another effect of the reports was to reinvigorate two existing but largely quiescent interagency bodies, the Interagency Intelligence Committee on Terrorism and the Interagency Group on Terrorism, which had been established in 1982. In 1985, following release of these reports and in the face of continuing terrorist attacks on U.S. targets, new attention was given to the idea that technological development had a significant role to play in protecting U.S. citizens and assets from the terrorist threat. The two interagency groups began to function more effectively, and each created a subcommittee on research and development.

In June 1985, TWA Flight 847 from Athens to Beirut was hijacked. In the course of that incident, a U.S. Navy sailor was brutally murdered, and the world's media were held enthralled for nearly 3 weeks while the drama played out. Following this event, President Reagan asked then Vice President Bush to chair a cabinet-level Task Force on Combating Terrorism. Reporting back in December 1985, the task force recommended, among other things, an effort to improve coordination among government agencies, creation of a full-time position on the National Security Council staff and establishment of a consolidated intelligence center on terrorism. This report further increased government interest in dealing with the terrorist problem in a coordinated way.

Since then, terrorist attacks on Americans and others have continued unabated throughout the world. However, until the 1988 bombing of Pan American Flight 103 over Lockerbie, Scotland, U.S. public attention to terrorism generally remained at a low level, apart from some peaks immediately following the 1985 hijacking of the cruise ship *Achille Lauro* and a few other incidents.

Lockerbie changed all that. That event revived deep public concern and resulted in calls for immediate action to protect U.S. citizens. Public opinion in other countries was also affected. This concern and interest has not gone away. Federal agencies, particularly the Federal Aviation Administration (FAA), were blamed for alleged laxity over the bombing and came under severe pressure to take major steps to improve security. Two advocacy groups, Victims of Pan Am 103 and Families of Pan Am Flight 103/Lockerbie, have been particularly effective in keeping the issue before the public and in demanding radical improvements in airline security.

In spite of increased public awareness, however, the United States (and, indeed, the world) continues to suffer terrorist attacks. Indeed, in late 1989, some terrorist bombings took place in the United States itself.[1] Major loss of life has also occurred in two 1989 airplane bombings in which some Americans were victims: UTA Flight 772 over Niger, en route from Ndjamena to Paris on September 19, 1989; and Avianca Flight 203 on November 27, 1989, just after take-off from Bogota on a flight to Cali.

In the summer of 1989, OTA was asked by three Senate Committees to study the state of research and development into technologies that could be of use in countering terrorism. Requests came from the Committee on Governmental Affairs; the Subcommittee on Terrorism, Narcotics, and International Operations of the Foreign Relations Committee; and the Committee on Commerce, Science, and Technology, with its Subcommittee on Aviation.[2] The three requests all asked for a study that would explore the state of research and development of technologies that could be useful in the battle against terrorism. The study was approved by OTA's Technology Assessment Board in September 1989.

The Committee on Governmental Affairs noted that the United States possesses a particular advantage in defending itself, its citizens, and its property: its high level of technological development. The Committee expressed the desire to:

> . . . assure ourselves that the Nation is taking full advantage of its capabilities in this area. While we are aware that there is no technical fix for terrorism, and that even the most ingenious technologies will not prevent all attacks, technology is a vital tool, to be used along with intelligence-gathering, law enforcement, and, where requested, military or paramilitary action.[3]

Letters from the first two committees asked for a broad assessment of relevant technology development, while the request from the Committee on Commerce, Science, and Transportation naturally focused more on counterterrorism as applied to airline security. In addition, this Committee also asked for information on the state of activities in the area of human factors, a field of study within the social sciences that deals with the effects of human behavior on systems. In this case, human factors would include items such as personnel training, ergonomics (the discipline that tries to optimize the interface between humans and machines), management techniques, improving mental concentration, and passenger screening by means of standard profiles.

The Committees also requested that OTA investigate the degree of coordination among the many agencies involved in counterterrorist work. A large number of executive branch agencies have interests and jurisdictions in counterterrorism, including some obvious ones (e.g., Department of Defense, the intelligence agencies, the Department of State, the Federal Aviation Administration, the Department of Energy, the Department of Justice, the Secret Service), and some not-so-obvious players (e.g., the Environmental Protection Agency). Assuring adequate coordination is a serious issue.

This report, the first produced by this assessment, gives an overview of Federal efforts to develop technical tools to aid in the battle against terrorism. It also provides a detailed discussion and analysis of technical aspects of research into explosives detectors, and gives the background of recent developments in the field. These are topics of great current interest, particularly when applied to airport security. Further, this report also covers research into technologies of use in other areas of counterterrorism: protection against chemical and biological attacks, physical security, data dissemination, and incident response. There is promising work taking place in all these areas. Some findings are presented along with some options for Congress regarding the funding of research and development and the implementation of some of the developed technologies.

The final report, due in the spring of 1991, will contain information on additional relevant technolo-

[1] In December 1989, two letter bombs were delivered in the southeastern part of the country. One killed a Federal judge in Alabama and another took the life of a Savannah, GA civil rights attorney. Other letter bombs, one sent to a Federal court building and the other to the headquarters of the National Association for the Advancement of Colored People in Jacksonville, FL, were defused. Racist letters claiming credit for the bombings were received shortly thereafter.

[2] In addition, a letter of endorsement for the study was later received from the Senate Select Committee on Intelligence.

[3] This and the other request letters are in app. F.

gies, and will treat areas not covered in this one. Among the items to be studied are: the role of human factors, weapons detectors, structural hardening of buildings and aircraft, systems approaches to physical security, detection of bomb mechanisms, and exotic weapons and sensors. Further discussions will analyze interagency and international coordination of research efforts as well as issues surrounding the efficient transfer of technology from the laboratory to the field. The topic of intelligence gathering will not be addressed in this assessment.

These reports represent further assessments by OTA in the field of terrorism, following an initial study, released by OTA in June 1990, which included an analysis of the vulnerability of U.S. electric systems to sabotage.[4]

PRINCIPAL FINDINGS

Finding 1

The Technical Support Working Group (TSWG) —the research and development (R&D) subcommittee of the Policy Coordinating Committee on Terrorism (PCC/T)[5]—is the only interagency coordinating group that has a broad perspective on the full range of technology development for fighting terrorism.[6] Many agencies perform such work, but each has a limited perspective related to its specfic mission. The purpose of TSWG is to provide seed money for important R&D that no agency has funded, usually because the area is outside the direct concerns of any single agency. When a TSWG project produces a successful prototype, appropriate agencies are to take on the role of further development and deployment. The broad agency participation is intended to maximize expertise and to assure that unnecessary duplication does not occur.

The downward spiral in funding the efforts of the Technical Support Working Group, from $10 million in fiscal years 1986-87 to $7 million in fiscal year 1988 to $3 million in fiscal year 1989 to $2 million in fiscal year 1990, has had a significant deleterious effect on counterterrorist research and development. The fiscal year 1990 number was the result of a compromise between the House of Representatives and the Senate, in which the Senate had tried to zero funding for the second year in a row. The TSWG could usefully allocate considerably more per year (probably up to $10 million) in worthwhile research for the foreseeable future.

Some successful and useful efforts are being uniquely performed under the aegis of TSWG. **They are in danger of being thwarted, due to low and declining funding constraints placed on this group.** There is no other government body with both the mandate and the practical ability to coordinate R&D efforts over the entire spectrum of counterterrorist technologies. Creation of the TSWG has greatly increased communication among scientists of the various agencies who often are working similar problems.

Moreover, in some areas of research undertaken by TSWG, there is apparently little government effort underway elsewhere. For example, it appears that virtually no other government agency has funded much research into developing responses to terrorist attacks of a chemical or biological nature.[7]

Several factors unrelated to the quality of the services performed by the TSWG have contributed to its fiscal vulnerability. Currently, its funding is lumped as a small item within the budget of the State Department's Bureau of Diplomatic Security. This reduces the profile of the TSWG and makes it more difficult for advocates to argue its case during the funding process. Also, since monies given to the TSWG are taken from the budget of the Bureau of Diplomatic Security, which has other major concerns, such as adequate security staffing, support for TSWG from within the State Department has not always been strong. **One option to solve the funding problem would be to provide a separate line item for TSWG in order to raise its profile for the purposes of budgetary decision making.**

Arguments to reduce or eliminate TSWG funding appear to center around concerns that it is not desirable to fund research out of State Department

[4]U.S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453 (Washington, DC: U.S. Government Printing Office, June 1990).

[5]The PCC/T is the successor committee to the Interagency Group on Terrorism, referred to in the previous section.

[6]Another group, the Interagency Intelligence Committee on Terrorism, has also recently begun funding R&D in the counterterrorism area, but focuses on technologies of particular interest to the intelligence community.

[7]An exception is a small ($200,000 per year) program run by the Army's Chemical Research, Development, and Engineering Center.

appropriations. However, this arrangement arose for historical reasons, in part because other agencies were reluctant to perform this role. The research is, however, managed by the Department of Defense, through the Naval Explosive Ordnance Disposal Technology Center,[8] which has the resources and experience to do so. Decisions are made by a broad interagency panel, so TSWG can only in a very narrow sense be considered a State Department research group. If, nevertheless, it were decided that the State Department should not be involved as the funding agency, one solution could be to place the funding in the hands of another of the member agencies, where participation in research is not in question. **If funding is to be crippled or eliminated, the decision to do so would more appropriately be made on the basis of arguments dealing with overall need or technical detail, not on institutional grounds.**

Several promising projects have been seriously delayed or halted because of inadequate or uncertain funding. The Transportable Emergency Response Monitoring Module is a case in point. The aim of this TSWG research program (managed by the Environmental Protection Agency and produced by Engineering Computer Optecnomics, Inc.) has been the completion of a mobile laboratory that can be deployed to the site of a chemical or biological attack, either threatened or real. This project has been delayed for a year due to lack of funding. Similar delays have occurred in a number of other areas. Payoffs, at least in some of these delayed projects, would probably come within 2 or 3 years if properly funded and supported.

In spite of these difficulties, TSWG has managed to bring several important projects from conception through to fruition. One example is the development of a portable protective hood, designed to be easily carried by officials who might be at risk of attack with chemical or biological agents. When donned, the hood encloses the head and provides temporary protection of eyes and airways until evacuation to a safe site can be achieved. A number of other projects are now nearing the prototyping stage.

Finding 2

Some promising areas of work in counterterrorist technologies are suffering from low or intermittent funding. A total of about $70 million, allocated specifically for research into and development of counterterrorist technologies, is spread across about 20 Federal agencies as shown in table 1-1.[9]

Apart from the general availability of Federal funds, two important, independent criteria are used to determine the level of resource allocation for research and development in a particular area: the importance of the work to national goals and the degree to which technological progress would benefit from funding. The first criterion is, in part, subjective. The second is more quantifiable, although with uncertainties that become larger, the further technical development is projected into the future.

While, in practice, it is difficult to justify the importance of R&D to national goals, the relative funding of various efforts affords a de facto measure of their relative importance. **The $70 million annual expenditure on counterterrorism R&D is roughly 0.7 percent of defense R&D at equivalent levels of development (including the defense 6.1, 6.2, and 6.3A items, i.e., research and early development). This provides a measure of the perceived importance of the effort relative to national security goals.** The counterterrorism R&D funding is also about 4 percent of the annual budget of the National Science Foundation and 3 percent of the fiscal year 1991 appropriation for the space station. This provides a measure of of its perceived importance relative to basic R&D budgets.

Some observers have suggested that since terrorism only affects the lives of a few hundred, or at worst, a few thousand persons per year—those of the victims and their families—the direct impact on the Nation is small. By this standard, as tragic as loss of life to terrorism may be, tobacco, other drugs, or drunk driving may pose much more serious problems for the United States. Such a point of view could support deemphasizing research into counterterrorist technologies and devoting more effort to solving those problems.

[8]This entity is managed by the Navy, but staffed jointly by all services to conduct R&D for the entire Department of Defense community.

[9]In addition, R&D in other fields (e.g., low-intensity conflict, counternarcotics) may produce useful products for counterterrorism.

Table 1-1—FY 1990 Levels of Federal Funding in Research and Development Specifically Directed at Counterterrorism (not complete)

Agency	Funding (millions of dollars)
Technical Support Working Group	2
Department of Energy	10[a]
Federal Aviation Administration	13
Naval Explosive Ordnance Disposal Center	4
Other Military Services	16
Other Department of Defense agencies	14
Others	about 10[b]

[a] Targetted almost exclusively against threats to nuclear facilities.
[b] Includes the FBI, the Secret Service, and the Customs Service. The relevant research budgets of these appear to be extremely low. The FBI, in particular, is unable to pursue many promising research projects, especially in the area of explosives detection, because of the minuscule amount of resources available (less than $100,000 per year).

SOURCE: Office of Technology Assessment, 1991.

Another point of view, however, holds that terrorism, beyond affecting the lives of many Americans, has also had a strongly negative effect on the ability of the United States to conduct its foreign policy, on the ability of U.S. businesses to operate and compete throughout the world, on U.S. prestige in general, and on the freedom of U.S. citizens to travel without undue fear in many parts of the world. From this viewpoint, terrorism is a pernicious scourge that affects U.S. national interests and national security far beyond its impacts on the lives of those most directly touched.

The "Irangate" affair provided a striking example of terrorism's ability to have serious and negative repercussions on the conduct of foreign policy, on U.S. prestige, and, potentially, on the U.S. military posture in the Middle East. A series of terrorist acts (i.e., kidnappings), was used by the Iranian authorities to extort policy changes from the U.S. Government (i.e., arms sales to Iran), which would otherwise have been rejected by the United States as inimical to its interests. Terrorism can have a multiplicative impact that is well beyond its immediate casualties.[10]

If it is decided that the threat of terrorism is more significant than indicated by the fraction of current military and other security-related R&D expenditures devoted to counterterrorist technologies, this would argue for an increase in resources. This does not imply that additional funds for R&D in countering terrorism should necessarily be taken out of the military R&D budget, which deals not only with terrorism, but all other military aspects of national security. Rather, the $40 billion for all military R&D indicates a scale of effort that is useful in helping to determine the appropriate level of effort for R&D into counterterrorism technologies.

The other consideration in determining the appropriate amount of R&D is the degree of maturity of the given research. Several important areas of R&D in counterterrorism are now funding-limited (i.e., progress is limited by available funding).[11] One example was noted under Finding 1, above. Appendixes A through D discuss a number of further examples of projects that have the promise of producing useful prototype instruments after a few years of assured and adequate funding.

Finding 3

OTA finds that requiring the mass acquisition of thermal neutron analysis (TNA) devices for installation at airports at this time is inadvisable.

In September 1989, the FAA established a rule outlining regulations that would eventually require the use of an Explosives Detection System (EDS) to screen checked (not carry-on) baggage in many airports serving U.S. carriers.[12] In this rule, the FAA Administrator was given the option of implementation at his discretion.

The only equipment currently deemed acceptable and approved as an EDS by FAA is based on a technique called thermal neutron analysis (TNA). The device was developed by Science Applications International Corp. (SAIC) under contract to the FAA Technical Center. This approval was given, however, based on restricted tests made under less than optimal conditions and without the concurrence of the Technical Center.[13] The machine uses low-energy neutrons to produce interactions with the

[10]Another example is the case of hijacked TWA Flight 847, in which the crew and hostages were finally set free in return for the promise (later carried out) of the release by Israel of a large number of arrested Shi'ites, some of whom had been involved in terrorist activites. It is a virtual certainty that some of those released again took up their interrupted task of terrorism. Thus, one terrorist act was able to multiply itself into many terrorist acts.

[11]R&D projects can be funding-limited or technology-limited. In the latter case, additional funding will not bring significant additional progress.

[12]Federal Register, Sept. 5, 1989.

[13]See Report of the President's Commission on Aviation Security and Terrorism, Washington, DC, May 1990, p. 65.

nuclei of nitrogen atoms (nitrogen is usually found in high proportions in explosives). As a result of these interactions, the nitrogen nuclei produce gamma radiation of a specific energy, which is detected and identified. The utility of this detector for finding bombs of the size that caused the Lockerbie crash has been widely questioned. A series of test results has confirmed doubts that the device would have a false-alarm rate low enough for practical applications.[14] Other proposed explosives detectors (some based on TNA and some not) that are available today in prototype or more advanced form are not yet more effective than the SAIC model, although many are smaller and those on the market are cheaper.

The rule was apparently established in response to strong public pressure and congressional action that led to the enactment of Public Law 101-45 on June 30, 1989.[15] The law requires the FAA Administrator to initiate action to:

> . . . require the use of explosive detection equipment that meets minimum performance standards requiring application of technology equivalent to or better than thermal neutron analysis technology . . . as the Administrator determines that the installation and use of such equipment is necessary to ensure the safety of air commerce. The Administrator shall complete these actions within sixty days of enactment of this Act . . .

The original TNA machine was not able simultaneously to: a) detect the smallest quantities of plastic explosives that could destroy an aircraft and b) maintain manageable false-alarm rates that would not hopelessly disrupt airline operations if it were used for all baggage.[16] Moreover, the exclusion of carry-on baggage from this rule provides immediate alternatives for the terrorist to pursue. Ironically, TNA would probably be more effective against explosives transported in carry-on baggage because the background coming from gamma radiation produced by innocent luggage would be less.

By itself, the original TNA device could not reliably protect against bombs like the one that brought down Pan Am 103, except to the degree that it might act as a deterrent to some terrorists. However, no other device for detecting explosives has yet shown itself more capable than the TNA system. It is possible, but by no means assured, that in the future, TNA or other technological tools will prove adequate to the task. However, no particular technology should be locked in until it works.

The resistance from airlines and airports to the FAA rule has demonstrated the difficulties that can arise from premature issuance of rules requiring corporations to make large expenditures to acquire devices that are operationally burdensome and of limited utility. Requiring installation of any device that is costly and complicates operations will naturally meet with institutional and individual resistance. This could be overcome if it were shown that the equipment added significantly to airline safety and security. If, on the other hand, it cannot be shown that devices that satisfy stringent performance standards actually exist, massive resistance to such rules, both from within the government and from the private sector, will persist. **This is the case today.**

If the costs for such devices become very burdensome to the private sector and if they are, nevertheless, deemed essential, an alternative solution would be government participation in funding. But if, as is the case, they are not capable of doing the required job, it makes no sense to deploy them.

There is a tradeoff: increasing security in a meaningful way will cost money and will likely raise operational difficulties for commercial air transportation. Congress and the American public will have to decide what level of expenditure and operational inconvenience is an acceptable cost for augmenting the safety of air travel.

On the positive side, well thought-out regulations should stimulate interest in developing useful technologies for explosives detection, since a potential market worth up to hundreds of millions of dollars would be created. This is what FAA tried to do, probably prematurely, in response to congressional mandate and public pressure.

---

[14]A false alarm is an indication by the machine that the object being surveyed contains a large amount of nitrogen in a relatively small volume, when the object actually contains no explosives.

[15]Some congressional staff feel that the passage of this law was based on miscommunication between the FAA and Congress regarding the perfomance capability of the TNA device—personal communication from staff of the Presidential Commission on Airline Security and Terrorism, June 15, 1990.

[16]There is a tradeoff between sensitivity and false-alarm rate. Reducing the threshold to detect smaller quantities of explosives increases the false-alarm rate significantly.

Testing a limited number of TNA machines at airports, as is currently planned and being done, serves a useful purpose, even if TNA turns out not to be the ultimate technical choice. The operational experience that will have been gained in applying explosives detectors online to passenger baggage under real conditions will provide invaluable information for devising specifications, standards, and practices for future systems. **Similar operational evaluation should be carried out for other promising technologies or for other versions of the TNA approach, whether or not the R&D was originally funded by FAA. Some other technologies,[17] as well as some other TNA manufacturers, should be candidates for such evaluations in the near future.**

Finding 4

Testing protocols for FAA's proposed Explosives Detection Systems (EDS) need to be established. Any acceptance test that will lead to mandated acquisition and use of a given device ought to use a testing procedure that is credible and acceptable.

Further, because of past problems regarding testing procedures, a testing authority independent of the FAA is urgently needed to sort out the divergent claims made by various sponsors of research and interested private corporations. After new testing procedures and authorities are established, the TNA device should undergo a new acceptance test to remain in consideration as one of the possible technologies. FAA has funded research in this area for several years. Because of its decisions during the last few years of funding research, the FAA is, correctly or not, perceived by many as having an institutional stake in particular technologies.

The FAA has been funding work on developing explosives detectors since 1977. Vapor sniffers for detecting explosives have been supported since 1984, and TNA development at SAIC has been sponsored since 1985. The increased effort in the mid-1980's was stimulated by various hijackings and terrorist incidents, especially by the bombing of an Air India flight from Montreal to London in 1985. FAA officials have reported an annual expenditure of about $8 million per year between 1985 and 1989 on explosive detector research.

In the fall of 1989, FAA issued a Broad Agency Announcement, asking for proposals for developing technologies in the area of airline security. Systems studies of combined technologies were specifically included in the announcement, as well as research into individual technological areas (e.g., explosives detection, metal detection, weapons detection, aircraft hardening against explosions). This positive step should expand the scope of FAA-sponsored research to include work to develop proactive technologies against future threats in contrast to previous R&D, which was largely reactive. **FAA should proceed to make this projected research program a reality as soon as possible.**

The TNA system prototype developed by SAIC was given "acceptance tests" at San Francisco and Los Angeles Airports in 1987 and 1988. These tests were devised in part by SAIC itself, were not double-blind (there was no attempt to conceal from the operators or observers which of the tested baggage had the explosive), and have been severely criticized by experts outside the FAA. They were designed to detect a minimum quantity of plastic explosive, an amount thought by some at the time to be a reasonable goal. The Lockerbie experience has indicated that a much smaller amount can bring down a Boeing 747. The design criteria of the apparatus and the acceptance test based on those criteria should therefore be considered insufficient. From this point on, any acceptance test for explosives detection should meet stricter criteria.

In early 1989, after the Lockerbie event, the FAA tested a vapor detection device in their Atlantic City Technical Center at the request of the manufacturer, Thermedics, Inc. A well thought-out, double-blind protocol was established that was stricter (although it used the same large quantity of explosives) than the original unblinded TNA acceptance tests. The device did not perform well in these tests, although in some cases plastic explosives were detected. The vendor then complained, not without cause, that their system had been called on to pass a test significantly more stringent than had the TNA device.

[17]Some examples are: a) computerized tomography, based on x-ray and computing technologies, that would produce a detailed three-dimensional image of an object; b) dual energy or back-scatter x-ray technologies that provide information on the atomic weight of objects as well as their densities; and c) vapor detectors that "sniff" the object, looking for molecules found in explosives. See ch. 4 and apps. A, B, and C.

As a first step to remedying this confusing situation, protocols for running the evaluation tests need to be formulated. Some possible candidate organizations that might be appropriate for providing protocols are the National Academy of Sciences, Sandia National Laboratory, Los Alamos National Laboratory, and the National Institute of Standards and Technology (formerly, the National Bureau of Standards). In the private sector, the American Society for Testing of Materials (ASTM) is also working on developing test standards. The FAA is currently trying to develop new protocols with the help of Sandia and an advisory board, including members from various agencies and the academic world.

Once protocols are established, the government should decide who will perform the acceptance testing. The past controversy over the acceptance of TNA has led to calls from many quarters for an independent testing authority.[18] Although nearly all observers agree that an independent testing authority is desirable to assure objectivity and credibility, there is less agreement on who that authority should be.

A choice acceptable to all stakeholders might be the National Institute of Standards and Technology, supported by an oversight board composed of representatives from the national laboratories, academia, and industry. Developing accepted standards for engineering equipment is one of NIST's historic roles. NIST has recently performed some testing in this area, but has not participated in any developmental work.

Another suggestion for a contractor to perform acceptance testing is Sandia National Laboratory, which has distinguished itself as expert in this field over the past decade. However, Sandia scientists have tended to focus on a limited number of detector technologies. Further, as a participant in explosives detector research and development, Sandia has a stake in the outcome in terms of allocation of research dollars. Proponents of other technologies might therefore feel disadvantaged if Sandia were to be the Nation's testing body for explosives detectors, in part out of a fear that those technologies on which Sandia has worked might be unduly favored. This reflects a common difficulty in such matters: if an institution has a long track record of work in a given area, perceptions may be that it has developed internal biases. Similar arguments might be applied to other National Laboratories, such as Los Alamos. The perception may not be accurate, but may still exist and cast doubt on the results of the testing. On the other hand, if the institution has little or no track record, perceptions are that its competence may be limited.

A further point concerns acceptance of any EDS at foreign airports. U.S. regulations require foreign air carriers to meet certain security criteria for those flights landing in the United States, under threat of revocation of domestic landing rights. Other countries may view U.S. regulations on the activities of their air carriers at their airports as violations of sovereignty. This problem could be eased by foreign participation in evaluation of candidate devices at an early stage. In general, international cooperation in both research and setting standards is essential to the establishment of effective security for international air travel.

Finding 5

Solving airline security problems will require not only technical equipment, but a systems approach that makes intelligent use of the technologies available. Immediate attention should be given to developing combined approaches to airline security that could be applied with current or near-current technologies as soon as possible.

As yet, no single explosives detector technology is adequate by itself against all reasonable threats. Until and unless a technological "magic bullet" appears on the scene, the civilized world must take what protective action it can with the means at hand. A role for TNA and other technologies in monitoring checked baggage may well be possible in this context. However, if properly sequenced, combinations of technologies from among x-ray, vapor detection, and nuclear techniques, such as TNA, may be much more effective, much harder to countermeasure, and much more of a deterrent to potential malefactors than any single method.

Additionally, since a large fraction of bombs planted on aircraft have been brought on board

[18]Statements of support for an independent testing authority have been made to OTA staff by an ex-Director of Security for FAA, by some vendors, and in public and private by FAA officials.

via carry-on baggage rather than in checked luggage, this path must be blocked as well. Efforts are needed to address in parallel the problem of detecting the introduction of explosives aboard aircraft by either route.

In addition to combinations of technical systems, the use of human factors techniques, such as enhanced security personnel training and supervision, along with methods of passenger screening, could play a strong role in improving security in commercial air travel. The apparent low level of activity in investigating the role of human factors—in developing passenger profiles, in human performance, and the man-machine interface—seems to be a weak link in R&D programs aimed at improving airline security.

Since the Lockerbie bombing, there has been strong public and Congressional pressure to upgrade airline security to improve significantly the security of the traveling public. This is natural, understandable, and reasonable. Airline security has been inadequate in dealing with the threat of surreptitious introduction of explosives on aircraft, particularly plastic explosives. These pressures explain the rush to mandate the use of the best device available.

However, current TNA equipment is expensive, bulky, time consuming, and (while the best device available) has definite limitations. Other currently available technologies may be cheaper and less bulky, but they are even less effective than TNA. Therefore, these other technologies should not yet be mandated either.

The difficulty is that no single current technology can yet, by itself, provide reasonable assurance of detection of bombs the size of the Lockerbie device, while permitting adequate throughput of passengers and baggage, and providing an acceptable level of false alarms. This is today's reality. Further, if one assumes relatively straight-forward efforts by terrorists to countermeasure detection devices, today's technology appears even less imposing. This may not be the case in the future, but the current state of affairs will last for at least a year or two, probably longer.

Until newer methods of detection are available, security could be upgraded in a number of ways.

- Additional procedures could be instituted and personnel hired to provide hand inspection of all suspect baggage. Improvements could be made in hiring, training, pay, motivation, and management of security personnel. Some efforts to this end have been made by FAA in concert with the Air Transport Association, an organization of commercial airlines. Whether these planned improvements are sufficient is not yet clear.
- Passenger screening by profiling could be greatly expanded, using interviews, as is done on El Al (Israel's airline) flights, and, in fact, is done on U.S. carriers in some locations.[19] These efforts would be labor-intensive and costly, but could be introduced reasonably rapidly.
- Security systems could employ simultaneously several less-than-perfect technologies that are now (or will soon be) available. Such a systems approach, combining different technologies, could be applied after some preliminary screening, would be far more difficult to beat, and would introduce great additional uncertainty for the terrorist.

In combining technologies, the strengths of some technologies could compensate for the weakness in others. For example, following screening by passenger profiles,[20] a fraction of bags could be selected for further investigation.[21] This might be followed by an x-ray device and vapor sniffer (far cheaper and smaller than TNA and smaller, cheaper, and quicker than tomography) that would pass on to a TNA or tomographic system only those bags that were still questionable. Finally, those bags still failing the tests could be fed to a device based on nuclear techniques that would finally prompt either the

[19]Although this has to be done in a competent fashion. A report on the Public Broadcasting System's television program, *Frontline* (Jan. 23, 1990), asserted that at least one interviewer in Frankfurt did not understand English, and although able to ask the questions phonetically, could not understand the responses.

[20]Security personnel might look for suspicious signals. There also may be patterns of behavior specific to "mules," those unsuspecting individuals who are deceived into unwittingly carrying explosives onto a flight. Research needs to be done into developing up-to-date profiles characteristics of both terrorists and unwitting accomplices, in terms of both general data and response to carefully selected questions.

[21]One possibility is the real-time matching of passengers with their luggage, so that no bag remains on the aircraft if the corresponding passenger is not on the aircraft as it rolls away from the gate. This is now required on international flights between the United States and certain foreign airports. This could be facilitated, for example, by barcode tagging.

opening of the bag in the presence of the passenger or else its disposal. In such a system, far fewer of the slower, expensive, bulky systems would be needed per airport, and the whole system would be a serious deterrent, since there would be so many different techniques for the terrorist to try to deceive.

This particular combination of devices is only meant as an example, not a suggestion for a workable airline passenger security system. The **point is, that with today's or next year's technology, a more effective and imposing system can be devised by combining several different ways of doing the same thing, rather than relying on only one technique.** Depending on false alarm rates, the total cost of such a system for a major airport could be less than requiring a TNA system to inspect every piece of checked baggage.

SUMMARY OF THE CURRENT STATE OF EXPLOSIVES DETECTOR DEVELOPMENT

The original TNA system cannot reliably detect bombs the size of the Lockerbie device with an acceptable false alarm rate. It is also very expensive per unit, and is large and heavy. Vapor detectors rely, in part, on surface contamination for detection, and, while some technologies, such as the chemiluminescence-based detector developed by Thermedics, Inc., are sensitive to plastic high explosives of concern, they are not currently sensitive to all explosives. There are, as yet, no reliable data on vapor detectors' ability to perform detection at satisfactory sensitivity in an airport environment.

X-ray techniques are too easily confused. They also have not yet been automated to the point where the machine can, without human intervention, reliably decide whether to pass an item or to sound an alarm, although some vendors are addressing this problem, and may succeed, to some degree, in the near future. Such automation has been mandated in the FAA rulemaking to eliminate too heavy dependence on decision making by the operators of the security devices, who are typically unskilled, poorly paid, and unmotivated. Computerized tomography is at an early stage and currently takes too long per bag for application by itself. However, one vendor, Imatron, hopes to demonstrate a solution to this problem in the near future. Like TNA, it will be expensive (although probably less so), large, and heavy.

There are several technologies that may possibly be ready for introduction in 1 to 5 years. Some of these are upgrades of previously mentioned technologies, which all (including TNA) can be improved. Computerized tomography may soon be in a position to play a useful role. There are others. The utilization of more energetic ("fast") neutrons, which could permit the detection of elements other than nitrogen (this element, or chemical radicals containing it, is currently used as the signature for nearly all explosives detection other than x ray),[22] may one day be practical at some level. With fast neutrons, carbon and oxygen could also be detected. Determining the ratios of carbon to nitrogen and carbon to oxygen would reduce false alarms and allow detection of non-nitrogen-containing explosives as well. Another technology that shows some promise is the use of high-energy gamma rays to probe for nitrogen nuclei by means of an enhancement in absorption of the rays at a well-defined energy. Many of these avenues may appear promising now but significant developmental work still needs to be done for each. In a following report, OTA will examine options for future FAA research programs in this field in more detail.

Only after prototypes are well tested in the field by independent authorities should the government mandate mass acquisition of equipment that would represent a major expenditure. However, initial steps to issue rules requiring equipment acquisition could stimulate a technology push, **if undertaken at a point when the technology appears to be close to meeting the requirements.**

[22]There are a few explosives that contain no nitrogen, although they are generally unstable and hard to handle.

Superintendent of Documents **Publications** Order Form

P3

Order Processing Code:
* 6978

Charge your order. It's easy!

MasterCard VISA

To fax your orders and inquiries—(202) 275-0019

☐ **YES,** please send me the following indicated publications:

_________ copies of ***Technology Against Terrorism: The Federal Effort—Summary (20 pages),*** S/N 052-003-01226-0 at $1.00 each.

☐ Please send me your **Free Catalog** of hundreds of bestselling Government books.

The total cost of my order is $_________. (International customers please add 25%.) Prices include regular domestic postage and handling and are good through 8/91. After this date, please call Order and Information Desk at 202-783-3238 to verify prices.

(Company or personal name) (Please type or print)

(Additional address/attention line)

(Street address)

(City, State, ZIP Code)

(   )
(Daytime phone including area code)

Please Choose Method of Payment:

☐ Check payable to the Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐–☐

☐ VISA or MasterCard Account

(Credit card expiration date)

Thank you for your order!

(Signature)

2/91

Mail To: Superintendent of Documents, Government Printing Office, Washington, DC 20402-9325

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a nonvoting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications; food and renewable resources; health; communication and information technologies; oceans and environment; and science, education, and transportation.

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT
WASHINGTON, D.C. 20510-8025

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
OFFICE OF TECHNOLOGY ASSESSMENT
379

U.S.MAIL ®

OTA-ISC-487

FEBRUARY 1991