Technology Against Terrorism: The Federal Effort

July 1991

OTA-ISC-487
NTIS order #PB91-219998
GPO stock #052-003-01246-4

TECHNOLOGY AGAINST TERRORISM

THE FEDERAL EFFORT

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT

Recommended Citation:

U.S. Congress, Office of Technology Assessment, ***Technology Against Terrorism: The Federal Effort, OTA-ISC-481*** (Washington, DC: U.S. Government Printing Office, July 1991).

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402-9325
(order form can be found in the back of this report)

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, and an unclassified summary was released to the public separately on February 26, 1991. 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 late 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. Maxwe11[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.
30, assignment from Sandia National Laboratories.
[4]On assignment from OTA's Science, Education, and Transportation Program.
[5]AAAS Fellow, 1989-90.

Contents

	Page
Chapter 1. Summary	1
INTRODUCTION	1
PRINCIPAL FINDINGS	4
Finding 1	4
Finding 2	5
Finding 3	7
Finding 4	8
Finding 5	10
STATE OF EXPLOSIVES DETECTOR DEVELOPMENT	11
Chapter 2. Introduction	13
THE ROLE OF TECHNOLOGY IN COUNTERING TERRORISM	13
OUTLINE OF THIS STUDY	13
Chapter 3. The Terrorist Threat	15
INTRODUCTION	15
A DEFINITIONAL FOCUS	15
TERRORISM: PAST, PRESENT, AND FUTURE	17
Historical Origins	17
Contemporary Terrorism	17
Two Decades of Terrorism: A Statistical Overview	19
Terrorism in the Future	19
THE THREAT TO THE UNITED STATES	23
Domestic Terrorism	23
International Terrorism	24
OBSERVATIONS AND CONCLUSIONS	28
Chapter 4. Research and Development	31
INTRODUCTION	31
Explosives Detection	31
Chemical and Biological Agents	32
Physical Protection	32
Incident Response	33
Data Dissemination	33
DETECTING EXPLOSIVES	33
Introduction	33
The Explosive Threat	34
History	35
Methods of Explosives Detection	38
Accelerator Technology	45
X-Ray Technologies	46
DEFENSE AGAINST CHEMICAL AND BIOLOGICAL WARFARE (CBW) AGENTS	51
Chemical and Biological Agents—Point and Remote Detection	52
PHYSICAL PROTECTION	54
Detectors and Alarms	55
Barriers	55
Building Hardening	56
Aircraft Hardening	56
Access Control	56
Baltimore-Washington International (BWI) Airport Project	57
INCIDENT RESPONSE	58
DATA DISSEMINATION	59

Chapter 5. Conclusions Regarding Current Research and Development Into Detection of Explosives 61
TESTING AND EVALUATION 62
MANAGING RESEARCH 63
Cooperation 63
Time From Laboratory To Deployment. 63
FAA RULEMAKING FOR EXPLOSIVES DETECTION SYSTEMS 64

Appendix A. Nuclear-based Explosives Detection Systems 67

Appendix B. X-Ray-Based Detection Systems 78

Appendix C. Vapor Detection Systems 81

Appendix D. Chemical and Biological Warfare Agent Detection 87

Appendix E. Recent Federal Counterterrorism Research Efforts: Agencies and Their Budgets . . . 91

Appendix F. Congressional Request and Support Letters 100

Figures

Figure *Page*
3-l. Distribution of Categories of International Terrorist Attacks 1970-79 and 1980-89 20
3-2. Geographical Distribution of Terrorist Attacks Against U.S. Citizens and Interests, 1970-79 26
3-3. Geographical Distribution of Terrorist Attacks Against U.S. Citizens and Interests, 1980-89 27
4-l. Densities of Various Materials 41
4-2. Nitrogen Percentage of Various Materials 42
4-3. Nitrogen Density of Various Materials 43
4-4. Correlation Between Oxygen and Nitrogen Densities in Explosives and Other Materials 44
4-5. Relative Volatilities of Some Common Explosives 48
5-1. Advantages and Disadvantages of Available (or nearly available) Explosives Detection Techniques 62
A-1. Sketch of Apparatus for Thermal Neutron Analysis of Nitrogen 68
A-2. Sketch of Apparatus for Fast Neutron Analysis of Nitrogen, Carbon, and Oxygen 71
A-3. Sketch of Apparatus for Pulsed Neutron Beam Analysis 72
A-4. Resonant Absorption of GammaRay s 74
A-5. Resonant Absorption of Garoma Rays 75

Tables

Table *Page*
1-1. FY 1990 Levels of Federal Funding in Research and Development Specifically Directed at Counterterrorism 6
3-1. Regional Distribution of Attacks Against U.S. Citizens and Interests 1970-89 25
4-1. Some Common Explosives 36
4-2. Explosives Detection Technologies 39
4-3. Airline Crashes Caused by Terrorist Bombs, 1982-89 40
4-4. Chemical and Biological Agent Detection Goals 53
5-1. Advantages and Disadvantages of Available (or nearly available) Explosives Detection Techniques 62
E-1. Federal Agencies Engaged in Counterterrorism Research 92
E-2. Allocation of FAA Security R&D Resources 98
E-3. Allocation of FAA Fiscal Year 1990 Contract Dollars for Major Program Priorities. 98

Chapter 1
Summary

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.

Photo credit: Washington, DC, Metropolitan Police Department and U.S. Capitol Police

Minor terrorism: debris from 1984 bombing of Washington, DC, Office of the American Civil Liberties Union, in same building housing the Off ice of Technology Assessment.

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

Photo credit: Federal Aviation Administration

Flight deck of commercial aircraft destroyed by terrorist bomb; Lockerbie, Scotland, 1988.

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

1111 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.

Photo credit: Federal Aviation Administration

Part of wreckage of commercial aircraft destroyed by terrorist bomb; Sahara Desert, Niger, 1989.

Photo credit: Federal Aviation Administration

Debris from destruction of commercial aircraft by narcoterrorist bomb; Soacha, near Bogota Colombia, 1989,

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 abroad 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 Environ-

[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.

mental 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 technologies, 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 I

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 specific 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

[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.

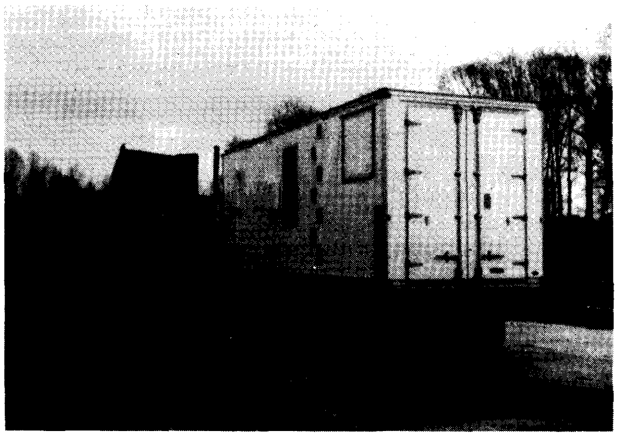


Photo credit: Engineering Computer Optecnomics, Inc.

Transportable Emergency Response Monitoring Module, for reacting to chemical or biological terrorist incidents, developed by Engineering Computer Optecnomics, Inc., under contract with the Environmental Protection Agency as part of the interagency research funded by the Technical Support Working Group.

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 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 domed, 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]

[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.

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 reemphasizing research into counterterrorist technologies and devoting more effort to solving those problems.

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.

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 IO[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). The Central Intelligence Agency refused to provide relevant information.

SOURCE: Office of Technology Assessment, 1991.

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.

[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.

The other consideration in determiningg 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 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

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

12Federal Register, Sept. 5, 1989.

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

14A false alarm is an indication b, 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.

15Some congressional staff feel that the Presage 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.

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

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.

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 manufacturer%** **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

[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.

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.

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

[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.

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 malefactor than any single method.

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

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

[19] Although this has t. 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.

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. Determiningg 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.

Chapter 2
Introduction

THE ROLE OF TECHNOLOGY IN COUNTERING TERRORISM

There is no technological fix for terrorism. It will never be possible to prevent all random, or nearly random, acts of murder and mayhem against innocent individuals or institutions, whether in the name of political or religious ideals or for any other cause.

A frequently expressed viewpoint holds that terrorism can only end when its root causes are dealt with. This point of view is not only defeatist, but without substance: the root causes of all terrorism will not be removed for a very long time. There are, across the world, persistent conflicting political, social, and economic claims. Moreover, there will probably always exist frustrated and unstable individuals, delighted to devise an ideological or theological excuse to commit unconscionable acts. Further, there are many instances where terrorism is employed on both sides of an issue. Ending the root causes of terrorism on one side could well aggravate the root causes on the other. In addition, for some states, terrorism has become a useful alternative way of doing business. These states have an interest in seeing terrorism continue.

These arguments do not deny the wisdom or legitimacy of efforts to satisfy real grievances among different groups of people in the world. But we should harbor no illusions of total and permanent success in ending terrorism by resolving political grievances, particularly in the near term. Meanwhile, common sense and common decency dictate a search for ways to defend the innocent from the depredations of the enraged.

It maybe impossible to end terrorism, but we can try to reduce our vulnerabilities (and, thereby, the likely number of terrorist incidents) to the greatest degree possible, consonant with the requirement to maintain a free and open society. Many terrorist acts, particularly those against transportation systems and against visible freed sites (e.g., embassies, military bases) can be deterred, prevented, or mitigated by judicious use of technological tools, when employed in conjunction with antiterrorist and anticriminal methods. Although not a fix, technology is and will continue to be a highly useful tool in the ongoing battle. It will probably play a far greater role in the future than it does today.

This report elucidates some of the means by which technology may be brought to bear on the problem of terrorism and provides some options for Congress to help facilitate the effort.

OUTLINE OF THIS STUDY

This OTA report is the first of two deliverables of this assessment. It includes, inter alia, a review of many relevant Federal activities and provides some details on the state-of-the-art for a number of fields of research. It also discusses the near-term prospects for deployment of useful tools in some of the better known areas of counterterrorist technology. It is, however, by no means complete. This study contains a detailed discussion of only a selected list of technical topics, although an outline of a good part of the Federal research is given.

Chapter 3 discusses terrorism in the world and in the United States from a historical perspective, to provide a basis for extrapolating the likely threat that will appear in the near and more distant future. As well as accounting for the progressive improvements that may be expected in technical sophistication of terrorist groups, particularly those with state sponsorship, decisionmakers must also allow for the very real possibility of qualitative changes in the terrorists' scope of activities.

While little, if any, terrorist activity has yet been manifest in the chemical or biological arenas, most observers agree that the technical capability for designing weapons based on these agents is not beyond the abilities of a large number of currently active terrorist organizations.[1] Given the availability of these weapons in the Middle East, there is the

[1] The use and production of chemical weapons by several states in the Middle East has been frequently reported in the press and, in part, by international observers, over the past few years. Such weapons were used by both sides, especially Iraq, in the recent Iran-Iraq War. In one case, Halabja in 1988, the Iraqis apparently were responsible for the deaths of thousands of Iraqi civilians by means of chemical agents. Another example of developing capability is the famous Rabta ''pharmaceutical'' complex in Libya, revealed by the U.S. Government in 1988, and the object of renewed international focus in March 1990.

possibility of a terrorist attack employing chemical or biological weapons in the near future. In fact, counterterrorist research is being undertaken by the Technical Support Working Group (see apps. D and E) to deal with this possible future threat. Chapter 3 discusses the topic briefly and the final report will examine the matter further.

Chapter 4 outlines many of the specific lines of research being pursued and discusses the prospects of near-term success for a number of technologies, particularly those dealing with detection of explosives. While not exhaustive, this section of chapter 4 provides a fairly comprehensive picture of the various possibilities for useful detection and the likelihoods of success for several approaches.

This chapter also discusses some work that has been done in the area of countering chemical and biological terrorism, both in the realm of early detection and portable protection and decontamination. An outline of ongoing work in several other areas is also included, such as barriers and alarms, weapons detectors, weapons neutralization, and data dissemination. There is also a discussion of efforts in the area of integrated airport security systems, which includes some of the technical topics discussed above as well as efforts to design effective systems from the technological components.

Chapter 5 presents some conclusions on research and development relevant to explosives detection, especially in the context of airport security.

The bulk of the technical analysis in this report is contained in appendixes A through D, which deal with explosives detectors, their variety, current capabilities, and the institutional, financial, and technical barriers to their immediate widespread deployment at airports around the world.

Appendix E presents an overview of Federal research in the counterterrorist area, from the perspectives of both individual agencies and inter-agency cooperation. It provides a quick look at the level of spending on R&D, giving the reader an overview of where most of the effort is going, both in terms of technology and agency. This view is not complete, in part due to the refusal of the Central Intelligence Agency to provide OTA with data and in part due to time constraints. However, it does provide a general picture of the level of intensity of related work and of the agencies involved.

There are two threats that will not be dealt with by either part of this assessment in great detail. One is nuclear terrorism, that is, terrorism that relies on the threat or use of either nuclear weapons or the dispersal of toxic radioactive agents. Since this topic has been widely analyzed in the last few years, and since research in this area (mostly funded by the Department of Energy and the Defense Nuclear Agency) has been very active and productive for well over a decade, this study will only touch on it. The other is attacks against computer systems. The matter of computer security against disabling attacks has not been considered a counterterrorist item until recently. There are many activities in this area, both in government and in the private sector. This topic is markedly different from other forms of terrorism and is being widely examined elsewhere. It is also a crime against property, rather than against persons (with some rare possible exceptions, such as attacks on hospital databases). Therefore, beyond a short mention, it will be considered beyond the scope of this assessment and will not be handled here.

Several technical and other topics are not covered in this report, but will be discussed in the subsequent one. One such topic includes the use of human factors studies and related sciences. Human factors have potential applications in:

- screening passengers at airports;
- motivating and assisting security personnel;
- dealing with crises, such as hostage-taking; and
- helping predict future activities of terrorists.

Another topic to be dealt with in more detail in the next report is the set of technologies useful in protecting freed sites, such as embassies, from attack. This includes barriers and access control technologies and techniques, and also the design and engineering of buildings and grounds to discourage attacks and mitigate them if they do occur. Yet other topics for further discussion in the final report include hardening technologies to protect aircraft and more exotic techniques (other than standard firearms and other usual weapons) for responding to hostage-holding incidents.

Chapter 3

The Terrorist Threat

INTRODUCTION

Political developments in 1989 and early 1990 throughout the world have led to a kind of euphoria that Americans have not known since the end of World War II. The tearing down of the Berlin Wall, the democratization of East European countries, and the decline of communism have been much welcomed by Americans of most political persuasions.

In addition to the developments in the communist world have been the recent changes towards democracy in other countries, such as the toppling of the Marcos dictatorship in the Philippines, the progressive installation of democratically elected governments in Latin America, and the winds of change in South Africa symbolized by the release of Nelson Mandela, the leader of the African National Congress (ANC), and the relegalization of the ANC and other anti-apartheid groups.

However, terrorism remains a vital threat to the security of the United States as well as other powers, large and small. The recent changes in the world have not diminished the dangers of terrorism—including new dangers created by the forces of extreme nationalism. Since the late summer of 1990, Iraq and its allied subnational groups have reminded us graphically of this.

This chapter presents perspectives on the nature, scope, and intensity of the terrorist threat affecting contemporary society and U.S. security interests.

A DEFINITIONAL FOCUS[1]

Many governments and peoples of the free world have failed to appreciate the magnitude and implications of the terrorist threat. Some democracies tend to regard terrorism as a minor nuisance or irritant. As a result, a large number of pluralist societies have not developed a strong commitment to deal effectively with the problem of terrorism.

A major reason for this failure is a definitional and moral confusion over what constitutes terrorism. The media, as the most critical instrument reflecting the perspectives of the perpetrators and opponents of terrorist acts, reinforce the confusion about terrorism.

It is prudent to distinguish among terms used to describe terrorism. Terrorism is perceived differently by perpetrators and by victims. To the attackers, whoever stands by a just cause cannot possibly be called a terrorist. . "[2] On the other hand, the diverse origins and semantic justifications of terrorist acts are irrelevant to the victims.

Moreover, the definitional focus of each sovereign government depends frost and foremost on the nature of its internal and external policies. Every sovereign state reserves to itself the political and legal authority to determine what is and what is not terrorism in the context of domestic and foreign affairs. For instance, the United Kingdom applies the term to the Provisional Irish Republican Army (PIRA), and Israel regards all violent acts by the Palestine Liberation Organization (PLO) as terrorist.

As a pluralist democracy, the United States speaks with a bewildering variety of voices on the subject of terrorism. Under the U.S. Federal system, each state determines what constitutes an offense under its criminal or penal code. An increasing number of States have defined terrorism generically as a crime, thus evading the need for use of specific statutes covering other selected criminal acts that are identified as terrorism.[3] Also, Congress has, over the past 20 years, held hearings, considered numerous bills, adopted resolutions, and passed laws on terrorism.[4]

---

[1]For sources on the definitional issues of terrorism as well as for literature on the general topic of terrorism, see, for example, Yonah Alexander (cd.), *Terrorism: An International Resource File, 1980-85 Index, 1986 Index, 1987 Index,* and *1988* Index (Ann Arbor, MI: UMI, 1986-89), and Edward F. Mikolus with Peter A. Flemming, *Terrorism, 1980-1987: A Selectively Annotated Bibliography* (Westport, CT: Greenwood Press, 1988). For a specific treatment of the issue of definition see, for instance, Brian M. Jenkins, "The Study of Terrorism: Definitional Problems" (Santa Monica, CA: RAND Corp., December 1980).

[2]Yasser Arafat at the U.N. General Assembly, 1974, as quoted by Secretary of State George Shultz in a speech in New York, Oct. 25, 1984.

[3]See, for example, Arkansas Criminal Code, Title 41, Sec. 41-1608, stating that "a person commits the offense of terroristic threatening if with the purpose of terrorizing another person he threatens tccause death or serious physical injury or substantial property damage to another person."

[4]See, for instance, H.R. 25o7 (101st Cong., 1st sess., May 25, 1989), a bill initiated to establish a commission On aviation security and terrorism, seeking to investigate the destruction of Pan Am 103 on Dec. 21, 1988, and KAL 007 on Aug. 31, 1983.

Nevertheless, a comprehensive working definition that can address the different forms of terrorist activity has not emerged from the Congress thus far.

Similarly, the executive branch, partly as a result of the very nature of its jurisdictional diversities, has not developed a coordinated position on the meaning of the term. For example, the Federal Bureau of Investigation (FBI) defines terrorism as 'the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. "[5] The Central Intelligence Agency (CIA), has specified that:

> . . . international terrorism is terrorism conducted with the support of foreign governments or organizations and/or directed against foreign nations, institutions, or governments.[6]

In recent years, however, both the Department of State and the Department of Defense adopted a definition that has been commonly used by the U.S. Government and which reflects:

> . . . a middle ground within the broad range of expert opinion, both domestic and international.[7]

Accordingly, State and Defense see "terrorism" as:

> . . . premeditated, politically motivated violence perpetrated against a noncombatant target by subnational groups or clandestine state agents, usually intended to influence an audience. "International terrorism' is terrorism involving the citizens or territory of more than one country.[8]

An analysis of these as well as numerous other definitions indicates that although there is a lack of consensus in public and private views on the subject,[9] the following elements are essential in what can be considered as "terrorism'

1. *Nature **of the Act: The*** concept of terrorist violence or threat of violence clearly embraces criminal, unlawful, politically subversive, and anarchic acts-piracy, hijacking of aircraft, taking of hostages, and other offenses of a political character.
2. ***Perpetrators:*** States as well as individuals and private groups may be perpetrators.
3. ***Strategic and Other Objectives:*** State sponsorship of terrorism is often part of a campaign of geographic expansion of political control. More recently, some terrorism has had as its political objectives the furtherance of illicit business operations. The prime example is the narcoterrorism waged by drug cartels in Colombia.
4. *Intended Outcomes and Motivations:* Fear, extortion, radical political change, and measures jeopardizing fundamental human freedoms of innocent parties are most often the expected immediate results. The ultimate goal usually is the satisfaction of political demands that the group does not feel able to achieve by conventional political, economic, or military actions. Terrorism is often born of such frustration.
5. ***Targets:*** Human beings and property are both targets of terrorist acts, with special focus on heads of states, diplomats, public officials, and military targets in noncombat or peacekeeping roles.
6. ***Methods:*** Threats, as well as the actual use of violence, including kidnapping, hostage-taking, and murder are the common weapons of terrorists in spreading fear among the targeted population.[10]

On the basis of the above components, it is reasonable to adopt the following as a working definition of terrorism:

The deliberate employment of violence or the threat of violence by sovereign states or subnational groups, possibly encouraged or assisted by sovereign states, to attain strategic or political objectives by acts in violation of law intended to

---

[5] U.S. Department of Justice, FBI, *Terrorism in the UnitedStates 1988* (Terrorist Research and Analytical Center, Counterterrorism Section, Criminal Investigative Division, Dec. 31, 1988), p. 34.

[6] "Pattern of International Terrorism: 1980," a research paper prepared by the National Foreign Assessment Center, Washington DC, p. ii. (This is a Central Intelligence Agency publication and is based on information available as of Dec. 31, 1980.)

[7] U.S. Department of Defense, *Terrorist Group Profiles (Washington DC:* U.S. Government Printing Office, 1988), p. viii.

[8] Ibid. See &w U.S. Department of State, *Patterns of Global Terrorism: 1988* (Washington, DC: March 1989), p. viii.

[9] See, for example, Alex P. Schmid, and Albert J. Jongman, *Political Terrorism* (Amsterdam: North Holland Publishing Co., 1988), pp. 1-39.

[10] Ray S. Cline and Yonah Alexander developed these elements in an unclassified report prepared for the U.S. Army on "State-Sponsored Terrorism" (1985), pp. 22-23.

create a climate of fear in a target population larger than the civilian or military victims attacked or threatened.[11]

Since terrorism represents the use of severe psychological and physical extra-legal force, typically directed against innocent victims, it is a violation of fundamental human rights, contrary to international law, and flouts the letter and spirit of the U.N. Charter and other relevant multilateral treaties.

TERRORISM: PAST, PRESENT, AND FUTURE

Historical Origins

Terrorism, as a cost-effective tool of low-intensity conflict that projects psychological intimidation and physical force in violation of law, has ancient roots. Mostly religious in motivation, terrorists systematically utilized swords and daggers during antiquity and the Middle Ages in their violent holy campaigns. Examples are the operations of the Jewish Zealot Sicarii, directed against Roman rule in occupied Judea as well as Jewish political and social enemies, and the martyrdom missions of the Hashashin (assassins), an offspring of the Ismailis, targeting the Crusaders and Sunni adversaries in Persia, Syria, and elsewhere in the Middle East. The former were active for 70 years in the first century and the latter lasted some 200 years-from the 1lth to the 13th centuries. Their experience has proven that terrorism can be attractive, effective, and durable, even if its tools are rather primitive.[12]

In subsequent periods, several European maritime states between the 16th and late 18th centuries employed pirates, or privateers, to terrorize the seas for the purpose of advancing foreign policy objectives. By the time of the "reign of terror" (1793-1794) during the French Revolution, terrorism from "above' and ''below' was commonplace. A variety of European groups nourished by anarchistic theories, left- and right-wing ideologies, and nationalism, have attained some tactical successes. Resorting to regicide and other terrorist activities such as bombing, extremists assassinated a considerable number of European rulers and ministers, including Tsar Alexander II in 1881. Although not intended by the perpetrator, the murder of the Austrian Archduke in Sarajevo drew the powers into World War I.

The period in the 20th century between the World Wars also witnessed terrorist violence in different regions of the world, such as Asia and the Middle East, where nationalist groups fought for liberation from colonial rule.[13]

Contemporary Terrorism

In the late 1960s, terrorism became a constant future of international life. Unique political circumstances led to this development, including the Six-Day War of 1967 and the rise of Palestinian terrorism worldwide; the adversarial relationship and physical proximity of the United States to Cuba, leading to numerous aircraft hijackings; the Vietnam War and the universal reaction against it; and the Paris students' revolt in 1968. These events, coupled with rapid developments in modern technology, communication facilities, and inexpensive and rapid travel, have contributed to the proliferation of indigenous and international terrorist groups and to the intensification of ideological and political violence.[14]

Another factor contributing to the expansion of contemporary terrorism is the role of certain states. A number of nations, such as Iran, Syria, Libya, and North Korea have sponsored terrorist operations as a form of secret or undeclared warfare in situations where overt or declared warfare would be inconvenient. Because modern weapons and all-out wars are

---

[11]Ibid., p. 37.

[12]See, for example, David C. Rappaport and Yonah Alexander(eds.), *The Morality of Terrorism: Religious and Secular Justifications* (New York, NY: Columbia University Press, 1989).

[13]See, for instance, Walter Laqueur, The Age *of Terrorism* (Boston, MA: Little, Brown& Co., 1987); and Walter Laqueur and Yonah Alexander (eds.), *The Terrorism Reader (New* York, NY: New American Library, 1987).

[14]For some general works on contemporary terrorism see, for example, Yonah Alexander (cd.), *International Terrorism: National, Regional, and Global Perspectives* (New York, NY: Praeger Publishers, 1976); Yonah Alexander, David Carlton, and Paul Wilkinson (eds.), *Terrorism: Theory and Practice* (Boulder, CO: Westview Press, 1979); Yonah Alexander and Seymour M. Finger (eds.), *Terrorism: Interdisciplinary Perspectives* (Maidenhead, England: McGraw Hill, 1978); and Robert Kupperman and Jeff Kamen, *Final Warning (New* York, NY: Doubleday, 1989). For an exhaustive survey of domestic and international groups see, for instance, Peter Janke, *Guerrilla and Terrorist organizations: A World Directory and Bibliography (New* York, NY: Macmillan, 1983); and Henry W. Degenhart, *Political Dissent: An International Guide to Dissident, Extra-Parliamentary Guerrilla and Illegal Political Movements* (Detroit, MI: Gale Research Co., 1983).

so expensive and destructive, these states, ideologically inclined to fight nations they perceive as enemies, may wish to restrict themselves to low-intensity conflict. In this mode, they attack their adversaries but confine their violence to the lower end of the spectrum of conflict, well away from the high-intensity of open, organized military hostilities. Since state sponsors of terrorism can engage in operations with little risk of being held accountable for their actions, they are usually not subject to reprisals by the target states.[15]

It is these political circumstances and technological and military realities that have led both subnational groups and state actors to employ violence or the threat of violence to attain political, social, and economic objectives in violation of law. As perpetrators, they became linked with each other. Many major terrorist groups around the world have at some point maintained a director indirect connection with a state sponsor. Some terrorist organizations appear to function at the exclusive service of certain states. In addition, over the past 10 to 15 years, collaboration among ideologically linked bodies and even among those without a common philosophy or political orientation has increased substantially.[16]

A case in point is the Japanese Red Army (JRA). JRA broke away from the Japanese Communist League Red Army Faction and established a distinct group in 1970. Aiming to form a People's Republic in Japan and to support a Marxist-Leninist revolution throughout the world, the JRA maintains ties with abroad range of movements inside and outside Japan. It has links with several other groups, such as the Popular Front for the Liberation of Palestine (PFLP), and maintains a base under Syrian control in Lebanon's Beka'a Valley. It also enjoys the support of Libya and North Korea and has set up terrorist cells throughout Asia, including Hong Kong, Manila, and Singapore.

The JRA has attacked, inter alia, U.S. targets, including American passengers at Lod Airport in Israel (1972); U.S. business facilities in Singapore (1974); U.S. embassies in Jakarta (1986), Rome (1987) and Madrid (1988); and a USO club in Naples (1988). Yu Kikumura, a JRA member, was arrested with explosives on the New Jersey Turnpike in April 1988 and was subsequently sentenced to 30 years imprisonment.

In addition to the JRA, other groups, acting independently or as surrogates for some states, have resorted to pragmatic and symbolic terrorist acts (e.g., arson, bombing, hostage-taking, kidnapping, and murder) for the purpose of producing pressures on governments and people to accede to the demands of the perpetrators. Their attacks have victimized, killed, and maimed large numbers of innocent civilians.

Terrorist acts have also inflicted considerable damage on targets other than people. Besides government offices and police stations, terrorists have attacked many property targets, usually those sites that either have many innocent persons present or have strategic importance (e.g., powerlines or pipelines).[17]

[15] See, for instance, Ray S. Cline and Yonah Alexander, *Terrorism as State-Sponsored Covert Warfare* (Fairfax, VA: HERO Books, 1986); *and* Yonah Alexander, "State-Sponsored Terrorism," *Harvard International Review,* vol. *7, No. 6, 1986,* pp. 21-23.

[16] See, for example, Yonah Alexander and Robert A. Kilmarx (eds.), "International Network of Terrorist Movements," *Political Terrorism and Business (New* York, NY: Praeger Publishers, 1979), pp. 34-56; and Claire Sterling, "The Great Bulgarian Cover-Up,"*The New Republic* 192:21, 1985, *pp.* 16-21.

[17] Chronologies of terrorist events used for this paper include a variety of sources, such as press indexes; FBIS; NEXIS; Facts-on-File; U.S. Government reports such as those published by the FBI, Department of Defense, and Department of State (e.g. Bureau of Diplomatic *Security, Significant Incidents of Political Violence Against Amen-cans, 1988);* annuals such as Yonah Alexander (cd.), *The 1986 Annual on Terrorism (The* Netherlands: Martinus Nijhoff, 1989); Edward F. Mickolus, Todd Sandier, and Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events, Vol. II, 1984-1987 (Ames, IA:* Iowa State University Press); yearly reports of terrorist events prepared by the Project on Low Intensity Warfare of the Jaffe Center for Strategic Studies of Tel Aviv University(JCSS), such as the latest publication INTER:*International Terrorism in 1988* (Jerusalem: The Jerusalem Post, 1989); the chronologies published by theRAND Corp. on different types of terrorism (e.g., Brian M. Jenkins et al., "A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets, " (Santa Monica, CA: The RAND Corp., September, 1983); and the information on terrorist attacks research by the Institute for Studies in International Terrorism, State University of New York.

Two Decades of Terrorism: A Statistical Overview

The statistics of both domestic and international incidents are startling.[18] During the decade of the 1970s, the total number of incidents worldwide was 8,114. There were 4,978 people killed and 6,902 injured. In terms of geographic distribution, Europe was the most active region, with a total of 3,598 incidents. Latin America followed with 2,252 incidents. The third region affected was the Middle East with 1,097 incidents. The most targeted victim during the 1970s was the business community, with a total of 3,290 incidents recorded.

The next decade was even more intensive in scope and destructive force. In 1980, 2,755 attacks were registered and their number increased to a record high of 4,422 in 1989, a 16-percent increase over the previous year. The 1980s saw a grand total of 31,426 incidents, with 70,859 killed and 47,849 injured, reflecting a lethality trend of more attacks designed to kill random victims. Figure 3-1 contains a summary of data on terrorist attacks.

Unlike the previous decade, in the 1980s the most violent terrorist region was Latin America, where 18,173 incidents were recorded. It is followed by Europe, with 4,613, Asia with 4,302, and the Middle East with 3,060.

Another approach to survey the nature, scope, and intensity of terrorism during the past two decades is to focus on its international character rather than deal with both domestic and foreign cases. According to the U.S. State Department database that records terrorist events involving the citizens or territory of more than one state,[19] the pattern of operations by subnational groups and state sponsors underscores a constant global rise in number of incidents.

In 1970, a total of 309 international operations were recorded; this figure more than doubled in two decades, reaching 661 incidents in 1989. overall, in the 1970s, a total of 4,234 international acts were perpetrated, with 2,783 killed and 4,799 wounded.[20] The primary target was the business community with 1,011 incidents recorded. Targets also involved diplomats (967), government officials (255), and the military (173)?

The decade of the 1980s marked a substantial increase in the number of international terrorist incidents and casualties. Overall, 6,501 operations were registered, with a total of 5,042 killed and 11,702 wounded. Shifting of the regional distribution of international terrorist incidents during the 1980s also occurred. Whereas in the 1970s Europe led the world in such incidents, the Middle East became the predominant location of international terrorist attacks in the 1980s. As in the preceding decade, the primary target of the 1980s was business with a total of 1,630 incidents.

Terrorism in the Future

In 1990, both domestic and international terrorism touched the lives and interests of individuals and nations in every region of the world. Some examples underline the diverse nature of recent incidents: a bomb exploded at the Chilean-U.S. Cultural Institute in Santiago; in Medellin, Colombia, a military judge was shot (one of very many murders there in recent years); a former Defense Minister was assassinated in Peru; and in Guatemala, a left-wing union leader from El Salvador and an activist were killed.

Elsewhere, a 1,000-pound bomb placed in a van exploded in Northern Ireland demolishing an unmanned police station and damaging 50 houses; Spanish deputies were shot in a Madrid restaurant; and a bomb killed two people and wounded two others in a bus terminal in Agdam, Azerbaijan. Also,

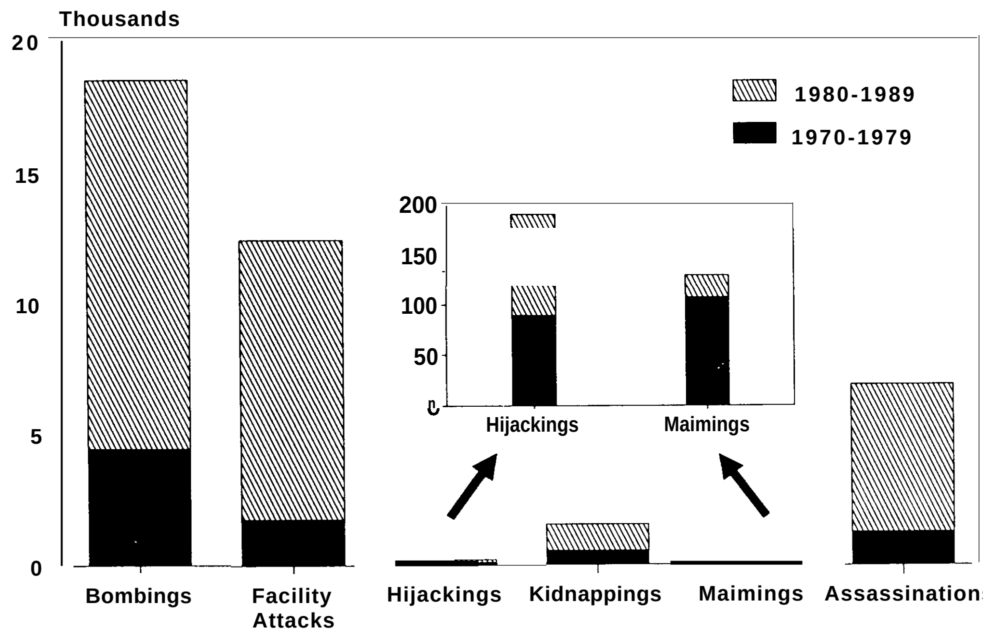
18Statistics on terrorism vary widely, mainly depending on the definitions employed by researchers. Numerous databanks focus undomestic terrorism, international terrorism, state terrorism, terrorism in specific countries, etc. Also, interpretation of these statistics differ, depending onthebody organizing the data. A major private statistical source for both domestic and international incidents is the database of Business Risks International (BRI) located in Arlington VA. It has issued monthly and quarterly reports since 1979, which are sold to subscribers. Some of the statistical material has been reprinted elsewhere in such publications as *Terrorism: An International Journal* and the annuals on terrorism, both edited by Yonah Alexander. The statistical material used in this section is drawn from BRI sources in dealing with both domestic and international terrorism. Other statistical databases consulted for this paper include JCSS and RAND materials.

19Available unclassified U.S. State Department figures cover the years 1968-1989. The statistical information for this period was provided by the *Office* of the Coordinator for Counterterrorism. Some of the statistical material is available in State Department publications such as *Patterns Of Global Terrorism,* op.cit., footnote 8, and *Significant Incidents of Political Violence* Against *Americans,* op.cit., footnote 17.

20According to the State Department data, the incident figures may exceed event totals due to overlapping.

21Ibid.

Figure 3-l-Distribution of Categories of International Terrorist Attacks 1970-79 and 1980-89



SOURCE: U.S. Department of State, 1990.

9 Israelis were killed and 17 were wounded in a tourist bus ambushed in Egypt; the Mayor of Nagasaki was wounded by extreme right-wing assailants; and a British member of Parliament was murdered by the Provisional IRA (PIRA). Towards the end of the year, the Speaker of the Egyptian Parliament was murdered by terrorists, and in 1991, the PIRA succeeded in launching a mortar attack on 10 Downing Street, disrupting a British cabinet meeting.

The Gulf War and its preliminary crisis brought several international terrorist groups together to offer their services to Iraq. In addition, a large number of (mostly minor) terrorist incidents occurred throughout the world after the onset of hostilities in 1991. Many of the latter attacks were apparently independent of Iraqi control and due to local, established terrorist groups that wished to express solidarity with Saddam Hussein and against the coalition nations.

While it is expected that similar kinds of incidents will occur in the forseeable future (i.e., terrorists will use a wide range of conventional weapons—guns, bombs, plus more sophisticated weapons, e.g., man-portable anti-tank rockets and surface-to-air missiles), the arsenal of tomorrow's terrorist might include instruments of mass destruction as well.

The specter of nuclear terrorism, such as the theft or detonation of a nuclear bomb, the use of fissionable material or intensely radioactive waste as a radioactive poison, or the seizure and sabotage of nuclear facilities, is seen by many experts as plausible and by others as inevitable.[22] At this time, however, more likely forms of nuclear terrorism would include a credible hoax involving a nuclear device, holding a nuclear facility or a shipment of highly radioactive material for purposes of political or economic blackmail, or dispersal of radioactive medical isotopes.

While the probability of a serious and successful nuclear terrorist episode remains low, the consequences in terms of mass destruction could be enormous. For example, if a crude, l-kiloton nuclear device (one-thirteenth the size of the Hiroshima bomb) were detonated (having been either stolen or built by a terrorist group with exceptional resources

[22]For detailed studies see Paul Leventhal and Yonah Alexander, *Preventing Nuclear Terrorism* (Lexington, MA: Lexington Press, 1987); and Paul Leventhal and Yonah Alexander, *Nuclear Terrorism: Defining the Threat* (McLean, VA: Pergarnon-Brassey 's, 1986).

and talent) in a major city, it could cause more than 100,000 fatalities and damage totaling billions of dollars. The human, physical, and psychological consequences of such an incident would be far more catastrophic than those of Three Mile Island (where there was no detectable loss of life but considerable financial damage) and the Chernobyl accident (which was caused by operators who overrode safety systems in a negligent, but not malicious reamer) which killed several dozen people outright, injured, or killed thousands of others, and caused severe property losses and untold damage to the environment.

Most experts agree, however, that it is easier to acquire the technical capability to produce chemical or biological weapons than it would be to produce or steal nuclear weapons. These weapons, like nuclear ones, are capable of producing enormous numbers of casualties in a single incident (perhaps up to several hundred thousand fatalities in a worst case, considering biological agents) and causing governmental and societal disruption of major proportions and widespread public panic.[23] Biological and chemical weapons have many advantages for terrorists. They include low cost as well as ease and speed of production; further, these weapons can, in principle, be developed by individuals with no more than a college-level education in the relevant field and with limited facilities. Weapons development requires only a minimum amount of tools and space, and equipment can be improvised or purchased without arousing suspicion.[24]

Further, many states are known to have chemical or biological weapons programs. The existence of the Libyan chemical weapons plant at Rabta has become common knowledge, especially since the fire at the site that at first was thought to have caused its destruction.[25] Besides this well-known chemical plant, chemical and biological weapons facilities exist in Iraq and chemical facilities have been reported in Iran. The development of such capabilities has been confirmed by leaders of both nations. The United States has developed chemical weapons, but decided to abandon the development of biological weapons.

Iraq and Iran have actually used chemical weapons on the battlefield.[26] Sixteen nations are known to have chemical warfare agents and another 10 are alleged to possess them.[27] According to publicly reported information, some 10 to 15 nations also possess an offensive biological warfare program. Will terrorist organizations acquire chemical or biological weapons, either on their own or from some state sponsor? According to some experts, the odds are perhaps even or slightly higher that such an attack will eventually occur.[28]

Terrorist organizations with a few skilled technicians (available to some terrorist groups for another task—bomb design) could easily amass the requisite capability in short order. Biological weapons are probably easier to develop technically and are more effective than chemical weapons. Because many biological agents persist and (if living agents) may multiply and spread, they can cause far-reaching epidemics. Thus, they should be considered to be a much greater potential threat than chemical agents.

A recent report prepared for the U.S. Armed Forces Medical Intelligence Center by the RAND Corp. discusses arguments for and against the likelihood of terrorist use of biological weapons.[29] In it, the technological barriers to use were not found

[23] See, for instance, Brian M. Jenkins and Alfred P. Rubin, "New Vulnerabilities and the Acquisition of New Weapons by Nongovernment Groups," in Alona E. Evans and John l?. Murphy (eds.), *Legal Aspects of International Terrorism* (Lexington, MA: Lexington Books, 1978) pp. 221-276; David Carlton and Carlo Schaerf, *The Dynamics of the Arms Race* (London: Croom Helm, 1975), pp. 170-93; and Jeremiah Denton, "International Terrorism: The Nuclear Dimension" paper presented at a Conference on Nuclear Terrorism, Washington, DC, June 25, 1985.

[24] See, for example, Richard Dean McCarthy, *The Ultimate Folly: War by Pestilence, Asphyxiation and Defoliation* (New York, NY: Random House, 1969); and Stockholm International Peace Research Institute, *The Rise of CB Weapons: The Problem of Chemical and Biological Warfare*, vol. 1 (New York, NY: Humanities Press, 1971).

[25] Later reports have cast doubt on the effects of the fire and even on whether the fire was real or a subterfuge that did little actual damage.

[26] See Seth Carus, *The Genie Unleashed: Iraq's Chemical and Biological Weapons Production* (Washington, DC: The Washington Institute for Near East Policy, 1989)

[27] U.S. General Accounting office, "Chemical Warfare: Progress and Problems in Defensive Capability," a report to the Chairman of House of Representatives Foreign Affairs Committee, GAO PEMD-86-11, July 1986.

[28] E. Hurwitz, 'TerrOriStS and Chemical/Biological Weapons," *Naval War College Review*, 35:36-40, *1982;* and H.J. McGeorge, "The Deadly Mixture: Bugs, Gas, and Terrorists," *NBC Defense and Technology International* 1:56-61, *1986.*

[29] Jeffrey D. Simon, *Terrorists and the Potential Use of Biological Weapons—A Discussion of Possibilities* R-3771-AFMIC, (Santa Monica, CA: The RAND Corp., December 1989).

to be ''insurmountable. The main problem to evaluate was the potential willingness to use such weapons, given their heinousness and the possible adverse reaction of the terrorists' own support base. Further, the employment of biological weapons is not as subject to user control as most other weapons and would require the terrorists to become familiar with a weapon technology that is substantially different from what they may be used to.

The RAND report concluded that some of the negative aspects of the use of biological weapons (from the terrorist perspective) might be becoming less important. The trend of mass killings through terrorist acts has been recently observed in multiple airline bombings, and one might foresee a reduced reluctance on the part of terrorists to take the lives of thousands of innocents since it has been demonstrably acceptable for them to take the lives of hundreds.

The use of chemical and biological agents by terrorists is not without precedent. For example, in 1978, a group identifying itself as the Arab Revolutionary Army Palestinian Commandos claimed they injected Israeli citrus fruit with mercury. An indication of the interest of at least one terrorist group in biological warfare was the factory for making botulinum toxin found in a raid on a hideout of the Red Army Faction in Paris in 1980.[30] Even in the United States, there have been incidents. One of the better known was allegedly perpetrated by a senior member of the Rajneesh cult in Antelope, Oregon in 1985, when among other similar incidents, bacteria were apparently used in an attempt to poison the food of a public official. And a few years ago, an extreme right-wing group, the Order of the Rising Sun, in St. Louis, MO, attempted to acquire the biological agent that causes typhus.

Biological weapons are, in some aspects, well suited to terrorist activities. They are small, easily concealed and transported, and readily activated. Some relatively crude forms are easily obtainable such as the common food poisons of salmonella, shigella, and staphylococcus, which can be procured from local clinical laboratories. They are readily grown in batches and can be dispersed in water. The extensive food and water hygiene and inspection practices of most industrialized countries might, however, complicate their effective use in food and water. Some agents can be dispersed as aerosols, but this requires greater skills on the part of the attacker.

State-sponsored terrorist organizations would appear to be the most likely to resort to biological warfare agents. They might have easier access to them; they could have the skills for handling and dispersing them and might wish to attack those targets most susceptible to such weapons, i.e., large populations in distant places, public buildings, or embassies. As noted above, several terrorist-sponsoring states have R&D programs in this domain. Of particular concern is a statement made by Iranian President H. Rafsanjani in a speech to "Islamic Fighters:"

> We should fully equip ourselves both in the offensive and defensive use of chemical, bacteriological, and radiological weapons. From now on, you should make use of the opportunity and perform this task.[31]

The examples of the attempted terrorist use of chemical and biological weapons in the past, statements on the part of leaders in some countries that are state sponsors of terrorism regarding the development of such weapons, and independent evidence on R&D efforts in some of those same countries, all indicate that the use of such weapons of mass destruction by terrorists in the future must be considered.

Although possession of such weapons by states that sponsor terrorism does not guarantee that the weapons or technology would be given to the terrorists, the possibility of such a technology transfer, whether intentional or not, cannot be excluded and should raise serious concerns. The recent example of the transfer of chemical weapons technologies from the Federal Republic of Germany to Libya indicates that such occurrences are possible even in a well-structured society with laws forbidding such behavior. Such transfers might be more difficult to prevent in less stable societies.

[30]Foreign Broadcast Information Service, Dec. 19, 1980, p. 8.
[31]Foreign Broadcast Information Service, Oct. 7, 1988, attributed to Tehran Domestic Radio Service, Oct. 6, 1988.

THE THREAT TO THE UNITED STATES

Domestic Terrorism

There have been occasional outbreaks of terrorism in the United States during the past 200 years perpetrated by both domestic and foreign groups. Some of the earliest "home-grown" groups include the vigilantes, originally organized to keep law and order in the lawless Western frontier; the Ku Klux Klan during the post-Civil War period; and the Molly Maguires, whose primary interest was vengeance against the anti-Irish-Catholic Scotch, Ulster, Welsh, and English Protestants in Pennsylvania during the 1870s.[32]

In the turbulent 1960s a proliferation of radical groups with violent tendencies occurred.[33] The Weather Underground, the New World Liberation Front, the George Jackson Brigade, the Symbionese Liberation Army, the Black Liberation Army, and the Black Panther Party, were among the most active of such left-wing groups in the United States during the late 1960s and 1970s. During the same period ethnic and nationalist groups (e.g., the Jewish Defense League, Armenian movements, Puerto Rican Armed Forces of National Liberation, Omega 7-Cuban Nationalist Movement, and the Cuban National Liberation Front) operated within the United States and Puerto Rico.

Although these groups have proved to be less professional and successful than their counterparts in other regions around the world during the 1970s, terrorist campaigns in the United States targeted the police, military, business, and other victims in over 600 attacks.[34] In justifying their operations, terrorists have communicated a multitude of rationalizations. For instance, in a statement claiming credit for the bombing of the Gulf Oil Building in Pittsburgh in June 1974, the Weather Underground explained that the attack was to punish the corporation for "financing the Portuguese in Angola, stealing from the poor in the U. S., and exploiting the people and resources of 70 countries. " The Jewish Defense League targeted Soviet facilities, residences, and vehicles as well as commercial firms or the installations of Eastern European countries in the New York area to protest the policies of the Soviet Bloc toward their Jewish minorities and Israel.

In addition to terrorism perpetrated by indigenous groups in the 1970s, foreign nationalist groups were also active in the United States. For instance, the Croatian group Otpor (Resistance) hijacked a TWA Boeing 727 from New York to Paris in 1976 to attract attention to its separatist goal of independence from Yugoslavia and took over the West German Consulate in Chicago in 1978 to demand the release of a Croatian leader in Cologne. The Secret Army for the Liberation of Armenia, seeking revenge for Turkey's genocide against Armenians during World War I, assassinated Turkish consular officials in Los Angeles during 1973. Also, the Black September Organization, operating within the framework of Fatah, the main group of the Palestine Liberation Organization (PLO) headed by Yasser Arafat, killed an Israeli air attache in Washington, DC, in 1973.

During the 1980s, the United States experienced fewer terrorist incidents domestically than abroad. According to FBI data, terrorist acts within the United States declined drastically after the first few years of the decade.[35] The total number of terrorist activities, both of indigenous and foreign origin, reached an estimated 220, approximately one-third that of the previous decade. The highest number of incidents were committed between 1980 and 1982 (122). Conversely, in 1989, only six cases were investigated as terrorist incidents, the lowest number in any given year during two decades of violence. A major reason for this encouraging trend has been the success of the proactive operations of the FBI and its

32 See, for example, Hugh Davis Graham and Ted Robert Gurr, *Violence in America: Historical and Comparative perspectives* (New York, NY: Bantam Books, 1970).

33 See, for instance, *Regional Risk Assessment: North America* (Alexandria, VA: Risks International, Inc., August 1979); ''Report of the Policy Study Group on Terrorism" (New York State: The Criminal Justice Institute, November 1985); and Brian M. Jenkins, "Terrorism in the United States, *TVI Journal*, vol. *5, No.* 1, 1984, pp. 1-4.

34 Ibid. See also Disorders *and Terrorism*, Report of the Task Force on Disorders and Terrorism (Washington, DC: National Advisory Committee On Criminal Justice Standards and Goals, 1976).

35 See Department of Justice, FBI, *Terrorism in the United States 1988*, op.cit., footnote 5, p. 11. See also statement by Oliver B. Revell, Associate Deputy Director-Investigations, FBI, before an open session of the Committee on Government Affairs, U.S. Senate, Sept. 11, 1989. For an overview of the domestic and international terrorist threat to the United States, see ''Public Report of the Vice President's Task Force on Combatting Terrorism, " February 1986.

effective cooperation with other law enforcement agencies in the United States and abroad. Prosecution of terrorists, such as the 1986 indictment by a Federal jury in Boston of eight radicals involved in a 9-year series of bombings, bank robberies and murder, has also been a contributing factor in the decline of domestic terrorism. Another factor has been a social phenomenon—the general loss of revolutionary fervor in the United States during this period.

To be sure, some of the terrorist groups operating in the 1970s were also active to some extent during the 1980s. There were left-wing groups such as the Weather Underground and the Black Panther Party, both involved in the Brinks armored car robbery in 1981 in Nyack, New York; the Armed Forces of National Liberation claimed 11 bombings in 1982. Also, the Jewish Defense League was active, engaging in violence against its perceived enemies.

In addition to these and other domestic groups, a variety of new bodies committed to ideological and political violence emerged during the 1980s. The most recent example of a group of terrorist attacks in the United States has been the series of letter bombs addressed to various lawyers and court officials in the southeastern United States at the end of 1989. A note claiming credit for the bombings implied racist motivations. Other examples of recent U.S. terrorism include reactionary right-wing movements advancing anti-Semitic and white supremacist causes as well as antigovernment and antitax beliefs (e.g., Aryan Nations) and the Evan Mecham Eco-Terrorist International Conspiracy (EMETIC), desiring to preserve the ecological systems by attacking perceived despoilers of the ecology through acts of sabotage ("ecotage"). Another example is the Animal Liberation Front (ALF) and related groups, dedicated to the elimination of animal use in medical research and industry. Animal rights groups in the United States have usually confined attacks to destruction of property, rather than humans. An exception, however, was the attempted murder of the president of U.S. Surgical Corp. by means of a bomb. In the United Kingdom, two animal rights bombings recently occurred-in one, a young child passing by was seriously injured.

Foreign groups have also continued their operations in the United States during the past decade. For example, the PIRA maintained a gun-running ring in 1982, and Sikh terrorists were prevented from destroying an Air India aircraft at Kennedy Airport in 1986 (although they had succeeded in Canada the year before). In addition, there is some evidence that foreign governments, such as Libya and Iran, have put in place in the United States an infrastructure to aid in carrying out terrorist acts. One possible example was the 1989 San Diego pipebomb attack on the car of the wife of Capt. Will Rogers, the commanding officer of the ***USS Vincennes,*** which had inadvertently shot down a civilian Iranian airliner with massive loss of life in 1988.

In short, although the general level of domestic terrorist activity has been reduced to relatively low proportions during the past decade, the potential for future attacks by both domestic and foreign bodies remains intact. One reason for this situation is the fact that many of the root causes of terrorism are perceived by potential perpetrators as being unresolved. Another factor is the inevitable emergence of new political, economic, and social problems that will encourage terrorism.

There is no evidence available to indicate that any U.S.-based terrorists have the intention or the capability to mount large-scale operations. Nevertheless, there are circumstances under which terrorism might escalate considerably within this country. For example, were the United States to intensify its war against the narco traffickers at home and abroad, terrorist acts in the United States could ensue.

International Terrorism

U.S. citizens and interests have been more affected by ideological and political violence abroad than they have at home. Indeed, during the past two decades, the United States has become a major target of acts of terrorism throughout the world. There are many factors contributing to this situation, including the fact that the United States maintains an extensive cultural, political, economic, and military presence abroad and that a considerable number of foreign groups and governments oppose American values, policies, and actions. This reality, coupled with other global developments such as technological advancements in weaponry and communications, has resulted in the expansion of international terrorist activities against the United States.

Statistical Data

Available statistics indicate the magnitude of the challenge to the United States. According to one nongovernmental database, the total number of international terrorist incidents directed against the United States during the past two decades was 1,617 (1970s—738; 1980s—879), with 915 killed (1970s—215; 1980s—700), and 1,149 wounded (1970s—314; 1980s—835).[36] The U.S. State Department's more extensive database offers a different set of figures.[37] According to it, during the same period, the total number of attacks against U.S. citizens and interests abroad reached 3,458 (1970s—1,705; 1980s—1,753), killings-722 (1970s—151; 1980s—571) and woundings-764 (1970s—227; 1980s—537) persons. According to the breakdown of U.S. victimization, the business community has been the primary target with 1,114 incidents registered, followed by the diplomatic community with 562 incidents, and the military with 438 incidents. Table 3-1 shows the number of attacks as a function of location; these data are also displayed in figures 3-2 and 3-3.

While the number of attacks has fluctuated, the overall percentage of the number of attacks against U.S. targets has risen sharply since 1975. For example, in the period 1975-79, attacks against U.S. interests abroad accounted for only 8.5 percent of the world total of terrorist incidents. In 1983, the percentage reached 35 percent of the world total, dropping to 26 percent in 1986, and slightly lower than 20 percent in the past 2 years.[38]

Targets and Tactics

An analysis of American victimization in international terrorist attacks in the past two decades demonstrates a wide range of civilian and military targets. For instance, every kind of U.S. business activity abroad has been affected, including financial (e.g., Merrill Lynch), banking (e.g., Bank of America), energy (e.g., Texaco), chemicals (e.g., Union Carbide), automobiles (e.g., Ford), communication (e.g., International Telephone & Telegraph), computers (e.g., International Business Machines),

Table 3-l—Regional Distribution of Attacks Against U.S. Citizens and Interests 1970-89

	Attacks		
Region	1970-79	1980-89	Total
Latin America	520	769	1,289
Western Europe	598	583	1,181
Middle East	274	148	422
Asia	138	172	310
North America	130	25	155
Africa	42	52	94
Eastern Europe	3	4	7

SOURCE: U.S. Department of State, 1989.

travel (e.g., American Express), and many others. In addition, every segment of the U.S. military abroad has been affected. The personnel, facilities, and operations of the Army, Air Force, and Navy have become a continuing target.

The tactics and tools utilized by terrorists in their attacks against U.S. targets overseas also varied widely in their nature. The following examples are typical:[39] incendiary devices (e.g., U.S. Government employees' cars in Greece, January 1973); mid-air explosion (e.g., Pan Am 103, Lockerbie, December 1988); car bomb (e.g., Occidental Petroleum, Bogota, February 1988); suicide truck bombing (e.g., U.S. Embassy Annex in East Beirut, September 1984); kidnapping (e.g., Lt. Col. William Higgins in Lebanon, February 1988); hostage-taking (e.g., U.S. Embassy in Tehran, November 1979); assassination (e.g., Assistant U.S. Army attache, Paris, January 1982); and hijacking (e.g., TWA 847, June 1985).

From these examples as well as from numerous other cases,[40] it is seen that terrorists attacking U.S. targets overseas have employed weapons and tactics ranging from primitive to sophisticated and modern. As far as the technological aspects of bombing are concerned, the devices ranged from home-made to advanced. For instance, at the primitive end of the scale, the components in an incendiary device employed in an attack on the American Cultural Center in South Korea in February 1988 included a plastic container, a desk clock, 9-volt batteries, and a chemical substance.

[36]Business Risks International annual reports, 1970-1989.

[37]State Department Statistics provided by the Office of the Coordinator fOr Counterterrorism.

[38]See James P. Wootten, "Terrorist Incidents Involving U.S. Citizens or Property 1981-1989: A Chronology," CRS Issue Brief, Aug. 11, 1989.

[39]Ibid. See also footnote 17.

[40]Information for these cases are derived from a variety of sources such as those cited in footnote 8, 17, and 19.

292-884 0 - 91 -- 2 : QL 3

Figure 3-2-Geographical Distribution of Terrorist Attacks Against U.S. Citizens and Interests, 1970-79

SOURCE: U.S. Department of State, 1990.

Such primitive devices, however, are increasingly being replaced by high-explosive bombs, often utilizing SEMTEX, a high explosive of Czechoslovak manufacture, or PETN, or other plastic explosives,[41] as starkly demonstrated in the downing of Pan Am 103 over Scotland in December 1988. Although current remote and timed detonator technology has advanced beyond the capability of some terrorist groups, many others have demonstrated the know-how to utilize sophisticated electronics to this end. Moreover, the probability is that more and more terrorist groups, both independent subnational and state-sponsored agents, will be employing sophisticated electronics in the near future.

It is also important to guard against the possibility of terrorists using such levels of technical capability in the near future, but in the realm of chemical or biological weapons rather than explosives and timers.

Perpetrators and Capabilities

Since the late 1960s, hundreds of subnational groups, acting independently or as proxies of state sponsors, have targeted the United States throughout the world. Some groups emerged for single-issue concerns such as the Frente de Liberation National de Vietnam del Sur in Argentina. Most of these are now defunct. Others, with broader goals, such as the Red Brigades of Italy, are still operational, though weakened.

The following is a selection of terrorist groups that have been active in recent years and have attacked U.S. citizens and interests:[42]

1. *Latin America:* Fuerza Zarate Willca (Bolivia); Simon Bolivar Command (Bolivia); Manuel Rodriguez Patriotic Front (Chile); M-19 (Colombia); Farabundo Marti National Liberation Forces (El Salvador); Guerrilla Army of the Poor (Guatemala); Shining Path (Peru); the Nicaraguan Contras; and unidentified elements within the military or security forces of El Salvador.
2. *Europe:* Red Army Faction (Federal Republic of Germany); Direct Action (France); Red Brigades (Italy); November 17 Organization (Greece); ETA or Basque Homeland and Liberty (Spain).
3. *The Middle East:* Al Daawa (Iran); Palestine Liberation Front (operating against Israel from

[41] See ch. 4 for a discussion of types Of explosives.

[42] See footnotes 17 and 19 for sources. See also Janke, op. cit., footnote 14, and Degenhardt, op. cit., footnote 14 for details on most of these organizations.

Figure 3-3-Geographical Distribution of Terrorist Attacks Against U.S. Citizens and Interests, 1980-89

SOURCE: U.S. Department of State, 1990.

bases in the Middle East); Hizbollah (Lebanon); Islamic Jihad Organization (Lebanon); Popular Front for the Liberation of Palestine-General Command (Syria); Abu Nidal Organization (Libya); Abu Ibrahim (15 May) Organization (Iraq).

4. ***Asia:*** Japanese Red Army (Japan); New People's Army (Philippines).

Terrorist groups often seek each other's support. For example, the PLO, through its affiliate members, such as Fatah, the Popular Front for the Liberation of Palestine (PFLP), the Democratic Front for the Liberation of Palestine (DFLP), Sa'iqa, and the Palestine Liberation Front (PLF), collaborated with numerous non-Arab groups, including the German Baader-Meinhof Group, the Italian Red Brigades, the Provisional Irish Republican Army, and the Japanese Red Army.

Individual members of the PLO have also been linked with Arab and non-Arab states. Thus, the PLF (headed by Abu'1 Abbas, who masterminded the 1985 attack on the *Achille Lauro* cruise ship, in which Leon Klinghoffer, an American citizen, was murdered) has received aid from Libya and Iraq. And the Fatah established a strong link with the communist bloc in an effort to create a vast infrastructure for undertaking terrorist activities throughout the world.

The latest shift in PLO policies, as expressed in the December 1988 renunciation of terrorism and the recognition of Israel, does not assure a complete disintegration of this network as long as forces opposed to PLO leader Yassir Arafat are committed to the "armed struggle" strategy. The recent abortive attack (which aimed at civilian targets) on Israeli beaches by Abu'l Abbas' Palestine Liberation Front provides a clear example of the persistence of terrorism from this quarter.[43]

The Hizbollah (also known by other names, such as Islamic Jihad), supported primarily by Iran, also maintains some ties with Syria, Libya, and the PLO. It has been responsible for some of the most spectacular terrorist attacks, including the bombing of the U.S. Marine barracks in Beirut in 1983, the hijackings of TWA 847 in 1985, and the kidnapping of most of the U.S. hostages in Lebanon.

The informal and formal relationship among various anti-U.S. terrorist groups and state sponsors has resulted in a machinery for terror on national, regional, and global levels. This framework has operated in many ways: ideological alliances, propaganda support, diplomatic assistance, geographic

[43]See, for example, Yonah Alexander and Joshua Sinai, *Terrorism: The PLO* Connection (New York, NY: Crane Russak, 1989).

sanctuary, financial help, training, organizational assistance, intelligence, weapons supply, and operations.[44]

A multitude of subnational groups and state sponsors have both the motivations and capabilities to continue to strike at U.S. interests abroad in the foreseeable future. In addition, the possibility also exists that foreign terrorist groups may try to attack U.S. interests even on U.S. soil, looking for targets that are among the less well defended. What is a particularly disturbing development is the trend in the instruments of terrorist warfare—from primitive arsenals into high-technology conventional and perhaps ultimately even unconventional (i.e., chemical, biological, or radiological) weaponry.

OBSERVATIONS AND CONCLUSIONS

In light of the record of the past two decades, the following observations and conclusions are offered:

First, terrorism poses a variety of threats to contemporary society. It has had a substantial impact on the way Americans live, work, and travel abroad. There is also an effect on the way Americans live at home. If there are attacks on U.S. soil (if, e.g., Kikumura had not been arrested by an observant State trooper on the New Jersey Turnpike and had succeeded in bombing populated sites in Manhattan), impacts will be far greater, particularly on the U.S. psyche.

Second, terrorism has become an integral part of the struggle-for-power process as a form of surrogate warfare, whereby small groups, with direct and indirect state support, are able to conduct political warfare at the national level, and ultimately may even succeed in altering the balance of power on an international level through, for example, the control of strategic resources in the Third World.

Third, terrorists operating today are better organized, more professional and better equipped than their predecessors of the past two decades. In the 1990s, it appears likely that they will be prepared to undertake greater operational risks. There is a very real possibility of attacks using chemical or biological weapons of mass destruction in the near future. This is of special concern since the **technology does not require a high level of education or training, and, in fact, such capabilities are possessed by a number of countries** that sponsor terrorist activities.

Fourth, a proliferation of subnational groups will continue to seek ideologically-based or single-issue goals. Their attacks in the future will be characterized by both continuity and change. Groups that are small and unsophisticated can be expected to continue to rely mostly on bombings. Those with enhanced skills and an international network will carry out more complex operations, **such as kidnappings, assassinations, and attacks on facilities closely associated with governments or companies whose policies the terrorists oppose.**

Fifth, a few of the more sophisticated terrorist groups will use increasingly high-leverage tactics to achieve massive disruption or political turmoil. Extremists will continue to operate as proxies or surrogates for particular governments such as Iran, Libya, and Syria. The techniques used will include more and more sophisticated technologies, particularly in the area of electronics, such as those used to provide sophisticated initiators, including remote-controlled ones, for bombs.

Sixth, **as some targets become more difficult for terrorists to attack, we can expect terrorist countermeasures to try to overcome added security systems as well as a redirection of effort towards less secure targets.** For example, there may be attempts to use surface-to-air missiles to attack aircraft when other means become too difficult to accomplish. Another possibility, again, could be the use of chemical or biological weapons.

Seventh, there are no simplistic or complete solutions to the dangers of terrorism. As the tactics utilized to challenge the authority of the state are and continue to be novel, so, too, must be the response by the instruments of the state. We must also be cautious to avoid the kinds of overreaction that could lead to repression and the ultimate weakening of the democratic institutions that we seek to protect.

Eighth, having achieved considerable tactical success during the 1970s and 1980s, terrorists sometimes find it politically expedient to restrain the level of political violence. These self-imposed restraints will not persist indefinitely, and future

[44] See *Terrorist Groups Profiles*, op.cit., footnote 7, and *Patterns of Global Terrorism,* op.cit., footnote 8.

incidents may continue to be costly in terms of human lives and property. Certain conditions, such as religious extremism or perceptions that the "cause" is lost, could provide terrorists with an incentive to escalate their attacks dramatically.

And finally, the vulnerability of modern society and its infrastructure, coupled with the opportunities for the utilization of sophisticated high-leverage conventional and unconventional weaponry, requires the United States both unilaterally and in concert with other like-minded nations to develop credible response capabilities, including the creation of adequate technological tools to minimize future threats.[45]

[45]For a discussion of a particular case of vulnerability, that of U.S. domestic power grids, *see* 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).

Chapter 4
Research and Development

INTRODUCTION

This chapter provides an overview of current research and development in technologies relevant to counterterrorism. The technologies are divided into several fields:

- detection of explosives and other weapons;
- detection of and protection against chemical and biological agents;
- physical protection (e.g., alarms, barriers, access control);
- incident response; and
- data dissemination.

Each of these functions is briefly discussed in this introduction and is detailed at greater length later in the appropriate section of this chapter.

Explosives Detection

One of the most important types of detector is the explosives detector, of great utility not only for airline security but also for the protection of fixed facilities, such as embassies, nuclear plants, or other sensitive buildings. The last 2 years have witnessed significant progress in explosives detection, both in commercially available (or nearly available) products and in R&D efforts. Another type of detector is the weapon detector, usually thought of as a metal detector (although this perception may change if other, nonmetallic weapons become available in the future). This report will not address weapon detection, which will be taken up in the final report of this assessment.

Explosives detector designs are based on a number of physical, chemical, and mechanical properties. One class of detectors is the "bulk' detector, which measures some of the physical or chemical properties of the object to be examined. Some detectors employ ionizing radiation to accomplish this: examples are detectors utilizing x rays, garoma rays,[1] or neutrons. Radiation is used to penetrate the object and the detector measures the outgoing radiation, which contains information on the details of the contents. This type of detector is limited in that, although it can be used on baggage, it cannot be applied to people because of the harmful effects of ionizing radiation at the intensities required by the widely available techniques. Recent progress in imaging objects using ''microdoses' of x rays may change is assessment. However, even if it could be rigorousl y shown that human exposure to microdose equipment would have negligible health effects, there would still be a severe problem in overcoming public skepticism toward the use of this type of equipment.

Another type of bulk detector uses nonionizing electromagnetic (EM) radiation in the form of radio waves. This includes high-resolution millimeter-wave radars that can search baggage or clothing for objects, such as explosives, that would scatter the microwaves. Also included are nuclear magnetic resonance (NMR) and nuclear quadruple resonance (NQR) spectrometers. These devices expose the volume to be searched to a pulsed radiofrequency EM field and then "listen" for pulse echoes characteristic of particular explosive compounds. Such detectors might be useful for consensual searches of persons for concealed explosives if the EM fields employed are sufficiently weak.

The vapor detector, or "sniffer," is a different class of detector. In this type of device, air samples are taken and examined by rapid chemical analysis techniques for the presence of molecules of explosive compounds. This class of detectors may well be used to search people as well as baggage.

The original vapor-based explosives detector is, of course, the dog, which is very effective for some purposes, but which has some serious "canine factors" limitations. Dogs, while very sensitive detectors, have limited attention spans, must be integrated as a team with a particular trainer to be most effective (thus generating high operating costs), and are often not consistent from day to day. They are still the best explosives detectors available for a wide variety of uses, such as a sweep of a well-defined area in the wake of a bomb threat. However, for many purposes, such as routine

[1]Garoma rays are, like x rays, electromagnetic radiation characterized by very short wavelengths, but unlike x rays, they are generated by nuclear, rather than atomic interactions. Gamma-ray wavelengths are generally shorter (equivalently, of higher energy) than x-ray wavelengths, but there is an overlap between the two types.

baggage inspection on airlines, dogs are not appropriate.

A host of factors, such as temperature, soak time (time between the placement of the bomb in the container and the attempted detection), amount of ventilation, and operator expertise, dramatically affect the performance of sniffers. Defining uniform, consistent, and realistic threat scenarios is critical to the development of minimum performance standards and objective evaluation criteria for vapor detectors.

Remote (or, in military jargon, "stand-off") detection of vapors is quite a challenging task. It could be particularly useful for examining, at a distance, vehicles suspected of containing a large amount of explosives. A laser beam, tuned to the correct wavelength, can be used to stimulate the molecules of a particular species of chemical vapor, for example, an explosive. These molecules then may absorb or emit light at well-defined wavelengths. These phenomena could form the basis of a remote detection scheme. The characteristic wavelengths of explosive chemical compounds would have to be systematically measured to provide a database for the detector. This type of technology is being developed for the detection of chemical warfare agents (see app. D). However, a relatively large amount of vapor would be needed in order to make explosives detection feasible. While the potential theoretically exists for applying this technology to the remote detection of explosives, small bombs in suitcases would not likely be easily detectable unless observed at very short range. However, there are other cases in which remote detection by laser absorption or excitation might be a possibility.

Another explosives detection mission, for different scenarios, is to look for buried explosives. Work is proceeding on the development of ground-penetrating radar that could find buried objects. This capability would have useful applications for a number of counterterrorist tasks, from finding buried arms caches to detecting mines.

Chemical and Biological Agents

A terrorist attack using chemical or biological (CB) agents has not yet occurred, but might happen in the near future (see ch. 3). The fact that such attacks have not yet taken place at a serious level (in a terrorist context) may explain the low priority given to efforts to analyze and deal with such eventualities. One exception to the general low priority given to this topic is the work undertaken by the interagency Technical Support Working Group (TSWG).

Sometimes referred to as "poor man's atom bombs,' chemical or biological munitions require far less technical sophistication than nuclear weapons. However, they, too, can qualify as weapons of mass destruction. It should be noted that classical chemical munitions and delivery technology were used effectively in World War I, some 75 years ago, and were further developed by several nations by the time of World War II. Some biological weapons technology is available, in principle, to any nation that can brew beer. Chemical or biological agents could be ideal for attacking targets such as embassies, perhaps through water or air supply systems.

Defense against terrorist CB attacks requires a combination of early detection and diagnosis, evacuation of endangered individuals, appropriate vaccines for preventing spread of infectious agents, antibiotics and antidotes for treatment, means of protection, and decontamination. An important element of defense against CB attack would be the ability to learn rapidly of the approach of such agents, either through air or water. Laser-based systems show some promise for early detection. Other areas of interest lie in the development of portable or miniaturized means of protection. There is some, but not much, activity in this area in the Federal sector. Some attempts to develop detection and protective capabilities applicable to terrorism have been made, notably by the TSWG.

Physical Protection

Physical protection includes the timely detection of attacks, delays forced on attackers (including armor and hardening of targets), and the response to attacks.[2] This section discusses alarms, barriers, access control to sensitive areas, blast protection, and hardening against projectiles. Detection and response are covered in other sections.

For example, physical protection for commercial airline security can include access control, applied

[2] Sandia National Laboratories, *Designing the Physical Protection System, vol.* **II of** *Physical Protection of Nuclear Facilities and Materials*, The *Ninth* International Training Course (Albuquerque, NM: Sandia National Laboratones, 1989).

both to passengers and site workers (this could amount to as little as a few locked doors with a security force able to respond rapidly); metal detectors; and, possibly, explosives detectors. A fully integrated system would also include perimeter design; division of the airport into different security areas, each with its own access control; closed circuit TV; various types of alarms; and barriers. In addition, aircraft could be modified or retrofitted to mitigate the effects of inflight explosion. Finally, human factors technology and related psychological research data could be employed, along with the mechanical components and defined system procedures.

General fixed-site security includes incorporating resistance to explosive blasts in architecture and engineering design, stand-off pedestrian barriers, and well-designed vehicle barriers. Further, as with airports, entrance procedures and access control for the public and on-site workers can present obstacles to a terrorist trying to introduce explosives into a building. In addition, external and internal barriers and protection devices are options for preventing overt assaults on a building.

Incident Response

Incident response covers those technologies useful in dealing with hostage-taking, an assault on a freed site, or other criminal undertakings that maybe interrupted by appropriate response force actions. Incident response includes disruption of the attack; defending targets, where possible; aiding the injured; protecting or evacuating those endangered; rescuing hostages; and apprehending the attackers. Coordinating different response forces (which may be from different agencies for a domestic incident or from different countries for an international case) is a key aspect of incident response.

There are many areas where technology or social science can help resolve the problem. For example, in some scenarios, pre-positioned sensors would be helpful in aiding rescue attempts. Human factors techniques, particularly applied to hostage negotiations, are vital in dealing with ongoing terrorist incidents. And software, ranging from checklists to sophisticated decision aides, would help. Incapacitating agents, riot control agents, or weapons that disable but do not permanently damage exposed individuals, might be of use in some cases. Possible techniques might involve chemical agents or exotic weapons using other physical principles.

The development of technology to aid various incident response tasks will be discussed in greater detail in the final report of this assessment.

Data Dissemination

Institutional and, occasionally, legal barriers prevent the free flow of information among Federal agencies, and among Federal, State and local law enforcement officials. This difficulty applies even where terrorist threats and time-critical information on terrorist activities are concerned. There are also some technical barriers to the rapid and secure diffusion of such information. On another level, it appears that even up-to-date R&D information is not always easily available to agencies that need it. Resolving this problem often requires modifying the behavior of institutions, although some technical developments could be useful in mitigating the situation.

This chapter deals with all of the above issues. In general, the information contained is not exhaustive, but provides an overview of the relevant technical work underway, along with an estimate of how near to field deployment the more promising technologies are. More details will be provided in the comprehensive final report of this study.

DETECTING EXPLOSIVES

Introduction

The detection of small quantities of explosives is often difficult but is by no means impossible. Advanced nuclear techniques and vapor detectors, as well as those based on other principles, have been refined to a point where simple detection is no longer the key issue: the question is rather whether the stringent demands of many applications can be met.

For example, there are several difficulties related to explosives detection for protecting commercial aviation. First, for screening baggage, the rate and volume of the load to be processed are daunting. U.S. airlines handle close to a billion pieces of baggage a year, and U.S. passenger traffic is over 40 percent of the total world volume. Therefore, the detection system must have a high throughput. The Federal Aviation Administration (FAA) requires a minimum rate of **600** bags/hour **(6** seconds/bag) for an explosives detection system, but airlines would like a screening rate at twice that speed for a given flight (a Boeing 747 typically ingests approximately **700** to **800** pieces of checked luggage). The ideal placement of a detection system for checked luggage would be at the check-in counter, where the passenger and bag are together, and where significantly more than 6 to 12 seconds are needed anyway for ticket processing.

Second, the threat is so diffuse. In 1989, only six baggage bombs were placed aboard aircraft (unless there were others that went undetected). It is not currently possible to err on the safe side by increasing detector sensitivity because too many false alarms would result, and the delays involved in resolving them would snarl the whole air traffic system.

Finally, many believe that explosives detection equipment must be automated (i.e., the decision to select a suspicious bag for further investigation is performed without human intervention), because inspecting many pieces is a repetitive and boring task of which humans (and even dogs) quickly tire, becoming inefficient. Still, in the end, the effectiveness of even the most highly automated security system will depend on the training and motivation of human beings-those individuals who perform further investigations.

While airline security involves searches of hand-held bags or packages, checked baggage, mail, and materials carried by individuals, other applications for explosives detection have different requirements. Inspection of vehicles, as well as packages or cargo, is a prime concern for other secure locations, such as U.S. embassies abroad. Searches must be rapid, cost effective, noninvasive, and nondestructive. There are a variety of techniques that can meet at least some of these criteria for some types of searches and produce a usable signal when encountering explosives.

Many techniques utilize ionizing radiation that penetrates the item to be searched. The radiation interacts with the nuclei of the examined object to produce absorption, secondary radiation, or both. These effects are then detected. Recent attention has focused on detection of nitrogen nuclei through nuclear techniques: nitrogen is found in high proportion in most explosives. There are various advanced versions of the common airport x-ray systems, as well as some chemical sniffers, each of which has specific capabilities and shortcomings. There are also techniques being investigated that utilize laser detection, infrared radiation, ultrasound, microwaves, and other methods that are not yet sufficiently developed to evaluate realistically.

This raises an important factor that differentiates among detection concepts: the relative state of their development. Experimental measurements have been made for a large number of different concepts. Laboratory systems based on some of these concepts have been used to demonstrate feasibility. A still smaller number have advanced to the prototype stage and have undergone actual airport experience. There are also some devices that are modifications of commercially available hardware systems and have new capabilities. Each of these categories must be viewed from a different vantage point with respect to their utility for the detection problem.

In general, devices that are in the research stage will be 5 to 10 years away from commercial availability, especially if they are based on new, complex technology. Worse yet, even this sluggish pace is premised on the assumption that adequate levels of federal support are forthcoming. A 2- to 3-year period may be expected for a successful research phase; a feasibility demonstration may well take 2 more years; a prototype program can easily last 2 to 3 more years; and, finally, any test at a customer site can take another 2 years.[3] Consequently, the status of each development program must be looked at carefully to assess where the concept stands in the development cycle. Hardware based on modifications of previously utilized products, which is sometimes possible with devices or systems used in other industries for other purposes, may shorten this cycle. As a rule, the simpler the device, the shorter the development time.

The Explosive Threat

There are literally hundreds of different types of explosives, varying from black powder used in pipe bombs (still a favorite of domestic bombers), to dynamite sticks, and from blocks of TNT to plastic explosives that can be molded into diverse forms, including thin sheets. A dozen or so of the most notable explosives, including most of those used by

3For example, the current thermal neutron analysis (TNA) technology is approximately 10 years old, with early research at Westinghouse predating the 1985-90 Scientific Applications International Corp. (SAIC) TNA program.

terrorists, are described in table 4-1. Of particular note are the explosives RDX and PETN which, together with plastic and other fillers, compose many plastic explosives such as Detasheet and SEMTEX.

History

Efforts to detect explosive materials have been ongoing for many years. Before applications for airline security were considered important, other applications (e.g., military security, security at nuclear weapons and nuclear power plants, security at the U.K. Houses of Parliament) stimulated interest in the development of explosives detection techniques. The use of dogs to sniff explosives has been common for over a decade, but there has been a simultaneous desire in the law enforcement community to find technical means of doing what dogs can do, doing it better, and doing it more consistently without the difficulties arising from canine factors, such as boredom, distraction, chemical maskers, mood, etc. Dogs as sniffers will be discussed further in the final report.

In general, detection techniques can be divided into two main categories: vapor detectors (relying on accurate identification of trace airborne samples of explosives) and bulk detectors (relying on an interaction between some kind of penetrating radiation and the hidden explosive). A list of various types of explosives detection strategies is presented in table 4-2 and a more detailed discussion is provided both later in this chapter and in appendixes A through C. A brief history of the development of these applications is presented below.

The first noncanine explosives detector, designed to sense dynamite vapor, was developed in the early 1970s by Analytical Instruments of the United Kingdom and its affiliate, Ion Track Instruments of Burlington, MA. In the two decades since then, progress has been great, and many competing techniques have been developed.

Interest in applying explosive vapor detectors to protecting commercial aviation increased after several terrorist incidents in the early 1980s, and FAA began sponsoring more research into sniffers in 1982. In 1984, the FAA funded Thermedics, Inc. of Woburn, MA to develop vapor detection technology in a direction that could prove useful for airport security. This work was aimed at producing a walk-through portal monitor. In 1986, the State Department also funded work at Thermedics to develop similar technology to detect explosives in packages. Earlier sniffer technologies were able to detect only those explosives with higher vapor pressures (1 to 100 parts per million), such as dynamite and nitroglycerine. Some manufacturers now claim that their products have been refined to the point where it is possible to detect TNT under realistic conditions. However, at least until recently, plastic explosives, which have far lower vapor pressures (as low as parts per trillion), were beyond detection by vapor means under conditions that would prevail in the field (i.e., at security portals or in airports). This situation has changed.

Researchers realized that detection of low vapor pressure explosives by sniffing techniques would be extremely difficult. Therefore, the FAA also funded efforts in researching nuclear techniques of detection, beginning with Westinghouse in the late 1970s and then, in 1985, also with a contract to Science Applications International Corp. (SAIC). This latter work led to the development of the Thermal Neutron Analysis (TNA) device that is currently the subject of much interest and controversy. The principal contract with SAIC on TNA was concluded in 1987 and 1988 with a series of 'acceptance' tests at the San Francisco and Los Angeles airports; SAIC was then awarded a contract to build five (later increased to six) TNA machines for installation and testing at various airports.

The TNA device is intended only for inspection of checked baggage, since it involves irradiating a test object with an intense "bath" of neutrons. In principle, it could also be applied to carry-on baggage, but, so far, cost and size problems, already a serious difficulty for the checked baggage application, have been cited as arguments against utilizing TNA for inspecting hand-carried baggage. In at least one foreign country, however, the feasibility of using smaller, less accurate, but cheaper TNA devices for this purpose is being explored.[4]

The problem of developing useful explosives detectors for commercial aviation security has increased in urgency and political visibility in the

[4]Since carry-on bags usually have less mass than checked baggage, it should be easier for a bulk detector, such as TNA, to see a small explosive in a carry-on item amidst the background generated by the rest of the luggage.

Table 4-l—Some Common Explosives[a]

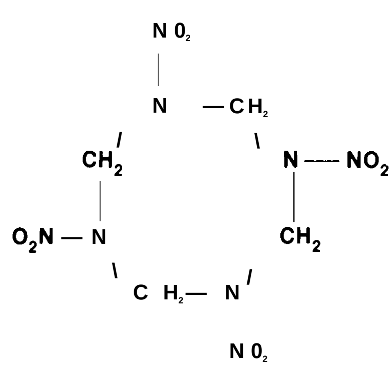
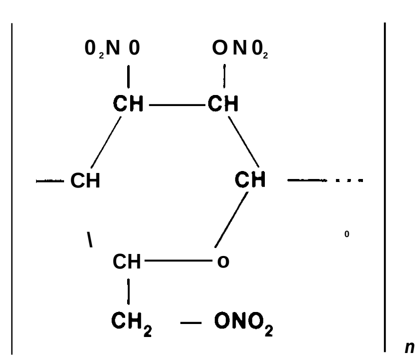
TRADE OF POPULAR NAME(S)	CHEMICAL NAME, FORMULA, AND STRUCTURE	COMMENTS
AN, Ammo-Nite	Ammonium nitrate $(NH_4)^+ (NO_3)^-$	Also commonly used as a fertilizer. Frequently mixed with fuel oil to make explosive called ANFO.
Black powder		Mixture of potassium or sodium nitrate, sulfur, and charcoal. Explosive most commonly used in terrorist bombs in the United States.
Composition B		60:40:1 mixture of RDX:TNT:wax
Dynamite		Compositions have varied over the years. The explosive components of modern dynamites are principally EGDN and NG absorbed onto combustible pulp (e.g., wood meal, starch, rye f l our),
EGDN	Ethylene glycol dinitrate H_2C-ONO_2 H_2C-ONO_2	One of the main components of dynamite. Quite volatile, making detection by "sniffers" relatively easy.
HMX, Octogen	Cyclotetra-methylene tetranitramine; 1,3,5,7-Tetranit ro-1 ,3,5,7-tetrazacyclooctane 	A military plastic explosive.
Nitrocellulose, gun cotton[b]		Main component of smokeless powder.

Table 4-1--Some Common Explosives[a]--Continued

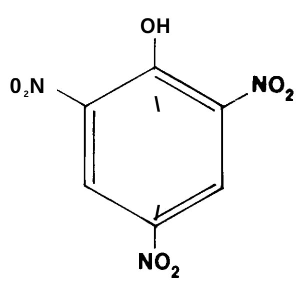
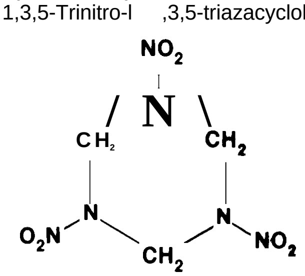
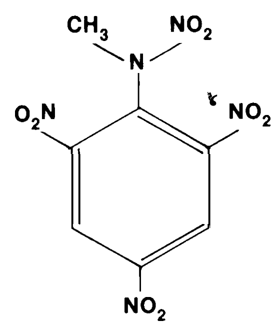
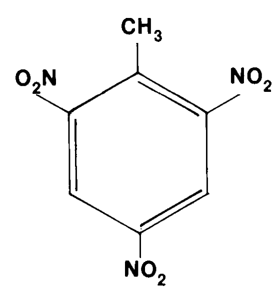
NG Nitroglycerine	Glycerol trinitrate H_2C-ONO_2 H! $CONO_2$ H_2C-ONO_2	
PETN	Pentaerythritol tetranitrate CH_2ONO_2 | O_2NOCH_2- C- CH_2ONO_2 | CH_2ONO_2	A plastic explosive available in bulk form or, with modifications, in sheet form under tradename "Detasheet." Unusually low nitrogen density for a plastic explosive: 18 percent by weight (compare with RDX).
Picric Acid	Trinitrophenol 	
RDX, Research Division X, Formula X, Cyclonite Hexogen	Cyclotrimethylenetrinitramine; 1,3,5-Trinitro-l ,3,5-triazacyclohexane 	Primary ingredient of military plastic explosives known as C-3 and C-4. 38 percent nitrogen by weight.
SEMTEX		**A** Czechoslovakian-made explosive composed of a mixture of varying proportions of RDX and PETN along with binder and plasticizer.

Table 4-l-Some Common Explosives[a]--Continued

Tetryl, Tetralite	2,4,6, N-Tetranitro-N-methylanaline; 2,4,6-Trinitrophenyl-methyl nitramine	Most common military booster.
		
TNT	Trinitrotoluene	A castable explosive.
		

NOTES:
[a] Much of the information in this table was derived from J. Yinon and S. Zitrin, *The Analysis of Explosives* (New York, NY: Pergamon Press, 1981), pp. 1-28.
[b] In practice, the nitration of cellulose is not complete and not all the OH groups of cellulose are nitrated.

wake of the Lockerbie crash, in December 1988. There had been previous bombings of aircraft, but most attacks on U.S. airliners, although causing some fatalities, had not brought down an aircraft. There had been several bombings that had destroyed non-U.S. commercial aircraft, the best known being the 1985 bombing on an Air India flight from Montreal to London, in which 329 were killed. However, none of these had the impact on the American public and Congress that the Lockerbie crash did. Table 4-3 shows major commercial aircraft bombings since 1980.

Following Lockerbie severe pressure was brought on the U.S. Government to take immediate action to prevent repetitions of this tragedy. The FAA, by virtue of its responsibilities and mission, bore the brunt of criticism and pressure for action. In addition, the media, some elected officials, and various private groups, such as the Victims of Pan Am 103, expressed the opinion that information constituting a sufficiently specific prior warning had been made available to some personnel in government agencies, while being concealed from the traveling public. This resulted in much public criticism of both the FAA and the Department of State.

Methods of Explosives Detection

All detection techniques depend on sensing properties that are shared by explosive compounds and are relatively unique to them. Fortunately, there are several physical, nuclear, and chemical characteristics of common explosives that are helpful to this end. Unfortunately, these compounds also share properties that make their detection difficult. The challenge to the designers of detection equipment is to create a system that can make use of the helpful properties and compensate for those that cause difficulties.

Table 4-2—Explosives Detection Technologies

Bulk detectors:
Using ionizing radiation
- **Nuclear**
  - **—Thermal Neutron Analysis**
  - **—Fast Neutron Analysis**
  - **—Nuclear Resonance Absorption of Gamma Rays**
  - **—Associated Particle Production**
  - **—Pulsed Fast Neutron Analysis**
  - **—Pulsed Fast Neutron Backscatter**
  - **-Nitrogen-1 3 Production with Positron Emission Tomography**
- **X-ray**
  - **—Transmission**
  - **-Backscatter**
  - **—Dual- or Multi-Energy**
  - **-Computerized Tomography**

Using non-ionizing radiation
- **Nuclear Magnetic Resonance**
- **Electron Spin Resonance**
- **Nuclear Quadrupole Resonance**

Vapor or residue detectors:
Dogs
Gas Chromatography (GC)/Chemiluminescence
GC/Electron Capture
Ion Mobility Spectrometry
Mass Spectrometry (two-stage)
Bioluminescence

SOURCE: Office of Technology Assessment, 1991.

The characteristics generally common to explosive compounds are:

- high nitrogen content and nitrogen density;
- the frequent presence of nitrogen as a nitro ($-NO_2$) group;
- high oxygen content, low carbon and hydrogen content;
- relatively high density (about 1.5 times the density of water);
- extremely low vapor pressure;[5]
- high polarity (also called electronegativity);[6]
- low thermal stability;[7]
- frangibility; [8] and
- adsorptivity.

Some nonexplosive materials have similar densities or percentage nitrogen content, but only a very small subset of materials has the high nitrogen density of explosives. Almost no nonexplosive materials have both the high nitrogen and oxygen densities that characterize most explosives.[9] A system that could reliably measure the nitrogen density distribution in a bag with good spatial resolution (probably one or two centimeters in each dimension or better), should be able to detect most explosives with few false alarms. One that could measure the distribution of nitrogen, oxygen, and carbon within a bag should provide detection with almost no false alarms.

Figures 4-1 through 4-4 illustrate this. Density alone, which is what the simple x-ray scanner measures, does not distinguish explosives from plastics and other common materials (see figure 4-l). Because certain fabrics contain a large weight fraction of nitrogen, the fraction of a bag's contents that is nitrogen is also not a good indicator of explosives (see figure 4-2). However, figure 4-3 shows that if the nitrogen density distribution can be measured locally within a bag, then only a very few materials will mimic explosives. Unfortunately, among these materials are melamine, leather, and solid nylon, none of which is particularly rare. These substances can cause false alarms if only nitrogen density is measured. Figure 4-4 shows how explosives could be identified uniquely by adding an oxygen measurement. Explosive detectors using nuclear techniques all utilize the above hierarchy of phenomena.

Nuclear Methods of Explosives Detection

One family of explosives detection devices depends on ionizing radiation, such as neutrons or high-energy photons (gamma or x rays), to penetrate the object to be inspected. The interaction of these penetrating types of radiation with the elements in the luggage produces signatures that can identify an explosive: the degree of uniqueness depends on the particular technique. The level of specificity of the

[5] If a large amount of liquid or solid is placed in a closed container, the material will evaporate until an equilibrium (also known as saturation) is established. Thereafter, the rate at which molecules escape into the gas phase will be equal to the rate at which molecules in the gas phase return to the condensed phase. The pressure generated by the gas phase molecules under these conditions is characteristic of the material and varies only with temperature. The more reluctant a substance is to evaporate, the lower the vapor pressure.

[6] Even though a molecule may be, overall, electrically neutral, atoms or groups of atoms within the molecule may be electrically polarized and have the power to attract electrons. This is called electronegativity. The $-NO_2$ groups typical of modern explosives possess this property.

[7] This means that the molecules easily breakup when their temperature is raised.

[8] Frangibility is the tendenc, of a molecule to break apart when it strikes Or is hit by another object.

[9] There area few non-nitrogen-based explosives, such asperchlorates. These, however, are relatively unstable and run the danger of exploding when the terrorist would rather they did not. To date, these have not been widely used in attacks on aircraft, although there is the possibility that if authorities were able to detect the nitrogen-based compounds, terrorists might turn to some of them.

Table 4-3--Airline Crashes Caused by Terrorist Bombs, 1982-89

Date	Airline/aircraft type	Route	Deaths
September 1983	Gulf Air/737	Karachi to Abu Dhabi	112
June 1985	Air India/747	Montreal to London	329
November 1987	Korean Airlines/707	Baghdad to Seoul	115
March 1988	BOP Air (South Africa)/ Bandeirante	Phalaborwa to Johannesburg, South Africa	17
December 1988	Pan Am/747	London to New York	270
September 1989	UTA/DC-10	Ndjamena, Chad to Paris	171
November 1989	Avianca/727	Bogota to Cali	101

SOURCE: Federal Aviation Adminietration, The Washington Post Counter-Terrorism and Security Intelligence, *Report of the President's Commission on Airline Security and Terrorism*, 1990.

identification is an inherent limitation on the usefulness of the concept. Other limits are the level of engineering development and the projected cost. The net utility of each method depends on its statistical probability of detecting hidden explosives of all sorts and on its potential for false alarms, which must be kept at a very low level (preferably less than 5 percent) to avoid disruption of normal operations.

TNA is unquestionably the most advanced of the current generation of Explosives Detection Systems (EDS), and, by virtue of the experience being gained at various airports, will also be the most tested. Nevertheless, the current SAIC TNA system, the only operational one, is, at best, a marginal EDS. It measures the presence of nitrogen by means of the interaction of thermalized neutrons (from a radioactive californium source) with the nitrogen nuclei. This interaction produces high-energy gamma radiation of a characteristic energy that is then detected.

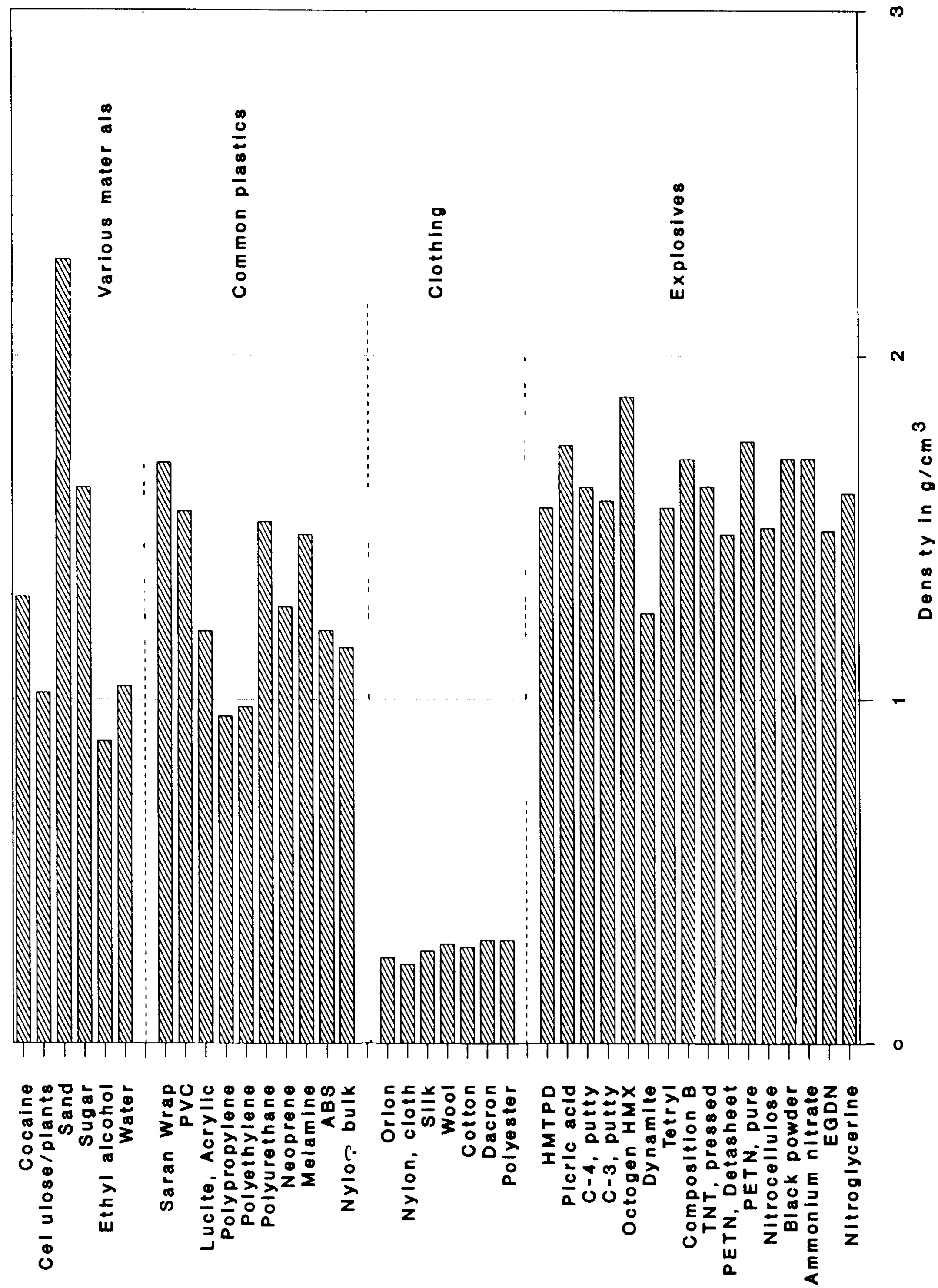
The numbers for detection probability and false-alarm rate vary, depending on several alternative details of the integrated detection system. Adding an x-ray device to TNA (utilizing and correlating information from both systems) and retrying suspect bags both change performance. Performance also varies with the type of baggage (defined by season, destination, and originating airport) being inspected. Its performance for detecting lesser quantities of explosives is poorer: the probability of detection is lower and the false-alarm rate higher. The FAA arranged for an outside group of experts to retest the SAIC TNA at more sensitive detection limits in early May 1990. See appendix A for a discussion of this test.

Checked baggage normally contains a wide range of nitrogen. The problem is to identify as suspicious only those bags with an excess of nitrogen-in an amount corresponding to the nitrogen content of a small plastic explosive-in the presence of this varying background. Attempting to detect smaller amounts of excess nitrogen would cause a large false-alarm rate. One possibility to resolve this problem would be to identify the location within a bag of any nitrogen excess. The current TNA has a limited spatial resolution, capable of giving only a vague idea of wherein a bag a suspiciously elevated nitrogen content is found, so its capacity for false alarm reduction is similarly limited. If TNA were to be applied to carry-on baggage, which usually has less mass than checked baggage, the background would be less and presumably the false-alarm rate for a given detection probability would be lower.

One of the unique features of TNA is that it is an automated system, i.e., one with no operator in the go/no go decision process. The system has some operational problems in that it does require significant shielding (built into the system) it is large and heavy, and is very expensive (about $1 million each). A more detailed discussion of the TNA concept is given in appendix A.

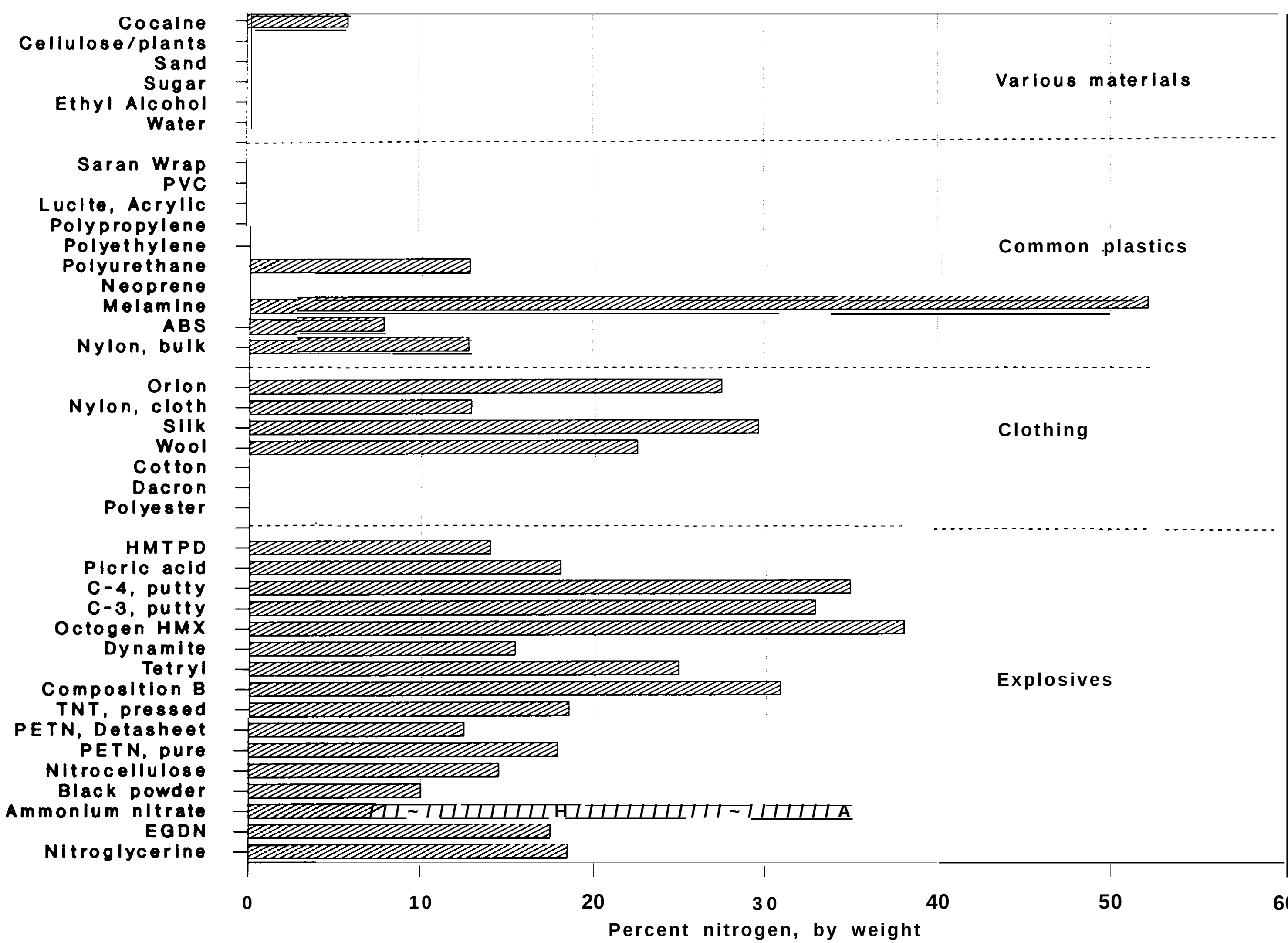
Beyond TNA, there are a number of nuclear-based systems that are in the laboratory demonstration stage. Several hold the promise of improving on some of TNA's shortcomings. One avenue of approach is to use faster neutrons, which allows the detection of elements other than nitrogen, such as oxygen and carbon, thus potentially reducing false-alarm rates considerably. The measurement of all three elements simultaneously would produce an effective and specific explosives discrimination process, as discussed above. Both steady and pulsed beam versions of Fast Neutron Analysis (FNA) are under investigation. Some concepts would greatly improve spatial resolution, as well as yield information on several elemental constituents of explosives. More energetic neutron systems require more complex sources, such as accelerators, which are not

Figure 4-1—Densities of Various Materials



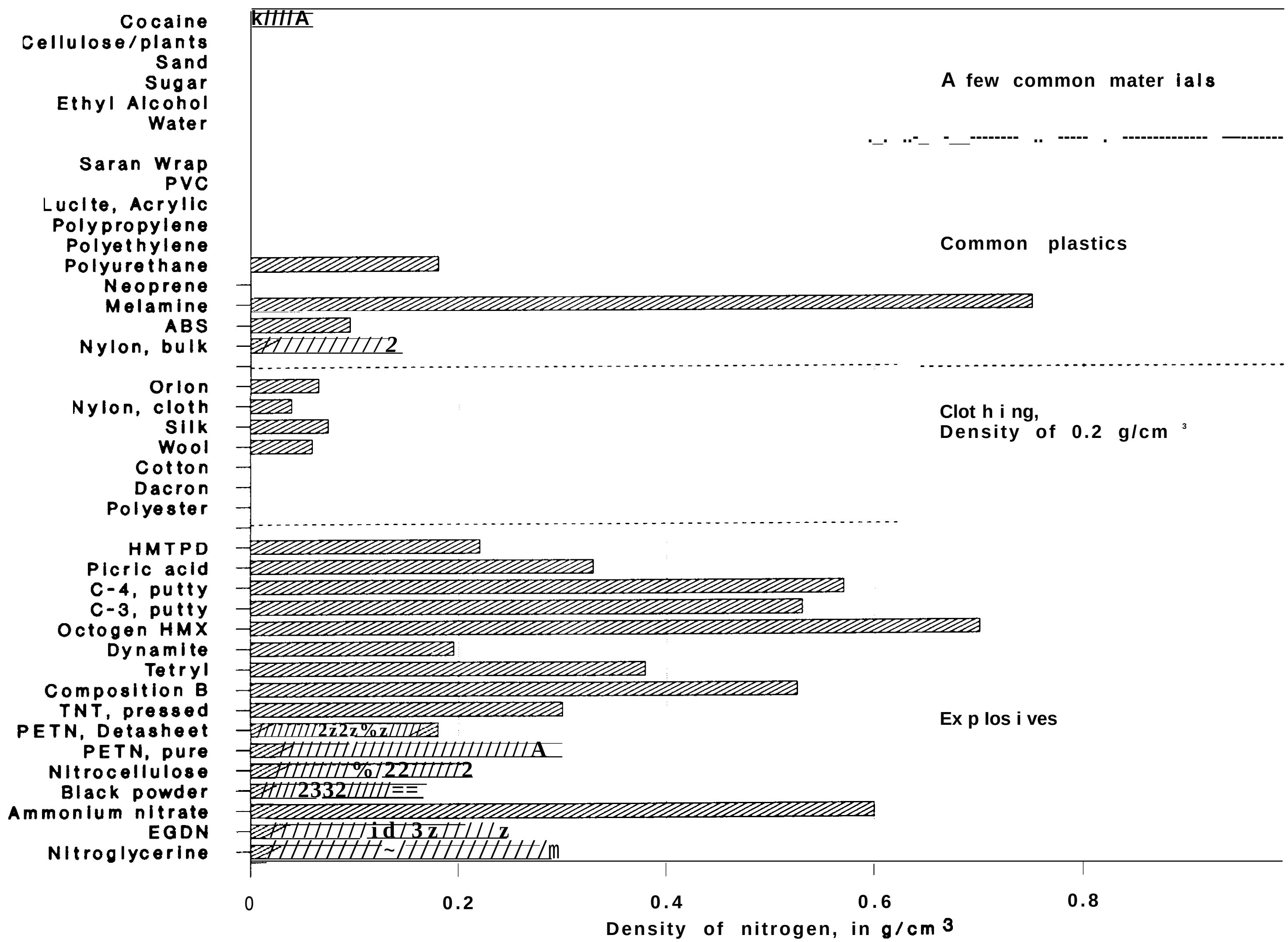
SOURCE: L. Grodzins, 1990.

Figure 4-2—Nitrogen Percentage of Various Materials



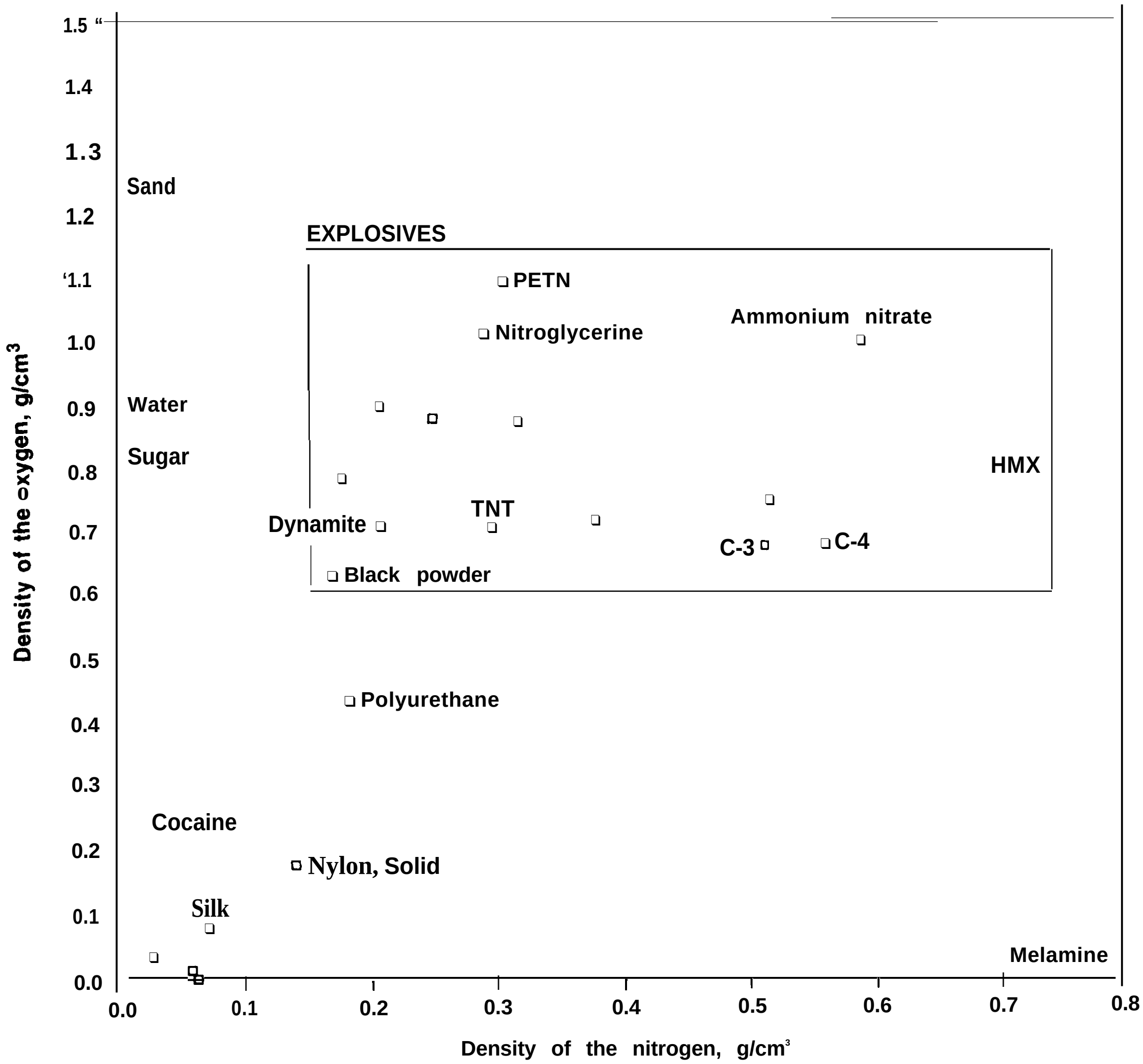
SOURCE: L. Grodzins, 1990.

Figure 4-3—Nitrogen Density of Various Materials



SOURCE: L. Grodzins, 1990.

Figure 4-4-Correlation Between Oxygen and Nitrogen Densities in Explosives and Other Materials



SOURCE: L. Grodzins, 1990,

available commercially and require development. Such devices will probably be larger, more expensive, and require more shielding than TNA. Appendix A discusses the FNA systems.

A somewhat different approach, based on the phenomenon of resonance absorption of garoma rays in nitrogen, has been explored and demonstrated in the laboratory and is now at the prototype development stage. In this approach, gamma rays (created through the absorption of a proton beam by a carbon target) are utilized to produce a gamma-ray absorption image that is specific to nitrogen content. The process has fairly good spatial resolution and is sensitive to small amounts of nitrogen, both advantages over the current TNA. However, OTA estimates that this concept is at least 3 years away from a prototype demonstration (if fully funded) of the sort currently being done for TNA. This approach is also described in more detail in appendix A.

There are several other nuclear-based explosives detection schemes, some of which are discussed in appendix A; a few other similar ones are not specifically mentioned. These concepts are all in the laboratory research stage.

Accelerator Technology

All nuclear techniques have a common problem in that they require means of generating neutrons or other energetic particles in order to produce the penetrating radiation with which they probe objects to be examined. All of the proposed techniques, with the exception of the current SAIC TNA machine that employs a radioactive californium source,[10] require some form of accelerator. Some general discussion of accelerator technology is thus useful to emphasize their common advantages and problems.

Although accelerator technology is a well-advanced science, work in accelerators has been primarily in support of laboratory experiments. Both small and very large machines are operated throughout the world, but generally by highly trained scientists, usually physicists or electrical engineers. An exception to this generality is in the area of semiconductor processing and medicine, where accelerators have been employed in industrial processes and where some success has been achieved in reducing their complexity and their costs of operation and maintenance. Fortunately, the accelerators needed for explosives detection are similar to those exploited for these applications.

Accelerators have common characteristics that complicate their use in industrial applications. First, they are complex, highly sophisticated machines, involving very high voltages (100,000 to 1,000,000 volts). Second, they are relatively large and take up a significant volume. Third, many produce neutrons, which must be stopped by shielding; further, most materials used to attenuate or isolate these neutrons are also activated and require their own shielding. The higher the energy and intensities of the produced neutrons, the greater the activation and shielding problem.

Another problem is that all accelerators require some source of ions or electrons, and these sources wear out. In general, the high current requirement and prolonged continuous operation of explosives detector applications tax the state of the art of these sources. Finally, all accelerator concepts that have been suggested for explosives detection will be considerably more expensive than the isotopic sources; accelerators would usually cost $100,000 and more.

Several different types of accelerators have been built or tested with an eye to eventual use for explosives detection. Early SAIC experiments for the FAA used a sealed source produced for industrial applications. This source was based on the D-D reaction, i.e., it accelerated a heavy hydrogen isotope, deuterium, to collide with a deuterium target. This source had a very poor lifetime (of the order of 100 hours). Later, under FAA sponsorship, an electrostatic accelerator was built (by National Electrostatic Corp.) and used at SAIC to replace the Cf-252 source in the TNA. It was judged too big, complex, and expensive ($200,000) by comparison with the isotopic source, but it has been successfully demonstrated as an alternative TNA source.[11]

The FAA and TSWG have also sponsored the development of another type of accelerator, the radio frequency quadruple (RFQ), which is currently under test by ACCSYS Technology, Inc. This system is a development based on Los Alamos National Laboratory technology (that had been advanced through funding under the Strategic Defense Initiative). The system was transferred to a small private company, which is continuing this research via a Small Business Innovative Research grant. Like all accelerators, the RFQ has the advantage of being switchable (i.e., it can be turned on and off at will). However, it is a pulsed system, which creates some electronic problems for TNA. It is unlikely that the RFQ accelerator can compete with the isotope source in cost, size, or simplicity.

Nuclear systems other than TNA require more energetic particles. Fast neutron analysis requires energetic neutrons. These are, in practice, usually of 14 MeV energy, generated from D-T reactions (in this case the deuterium target is replaced by a tritium one--tritium is a radioactive isotope of hydrogen). Although so-called electronic tubes to produce these reactions have been available for scientific and some industrial applications (e.g., for well-logging in the oil industry) for years, their development for explosives detection is still in prototype testing stages

[10] The californium-252 source used in the SAIC TNA was a judicious choice from several points of view: it is used extensively in the medical field and in other industrial applications; it is well developed and industrial qualified; highly tested models are available; it is very small compared to most accelerators; its shielding requirements are well known; and it is relatively inexpensive ($10,000 to $20,000). However, its radioactivity introduces its own set of problems and concerns, which have been discussed.

[11] W. Wall, FAA Technical Center, personal communication, 1990.

(e.g., at SODERN in France). The operating characteristics of such devices have not yet been assessed. Such systems are being developed to support both the continuous and pulsed version of fast neutron analysis.

Other techniques, such as nuclear resonance absorption (NRA) of garoma rays, have special accelerator requirements. In the NRA case, a relatively low energy (1.75 MeV) proton beam is required. This eases the shielding requirements because few nuclei will be rendered radioactive by such a low energy proton beam. However, the systems requirements, particularly in terms of beam current (the number of protons produced per second), do strain the state of the art of this type of accelerator. Electrostatic accelerators, similar to laboratory Van de Graaff high-voltage machines, can support early NRA experiments by extending the present current-carrying performance of the systems and sources by a factor of 2 to 5 (to about 0.5 milliamperes (mA)). It is believed that a final system would require currents beyond this capability (2 to 5 mA). Other accelerator candidates are available, based on concepts that have been used in industrial ion implantation machines, but the development and industrialization of such accelerators has been a time-consuming, multimillion dollar program.

Still another class of accelerator under consideration is the electron accelerator needed for the Nitrogen-13 production concept. In this case, a radiofrequency (RF) linear accelerator (LINAC) is the prime candidate. Production of a 13.15 MeV RF LINAC of sufficient current is not a great challenge to the technology. The issue is one of size, shielding, industrialization, and cost. From current experience, it is not likely that such a system will be small, easy to shield with minimal structure, or cheap.

X-Ray Technologies

Existing commercial x-ray scanners are capable of giving high resolution images of the interior of objects. They have been used for many years to check hand-carried baggage and, more recently, checked luggage. During the last 5 years, major strides have been made in x-ray technology. New models are far more capable than those in general use at airports today. Some of these new systems can now differentiate between materials composed of light or heavy elements, and some have very good resolution with three-dimensional imaging capability. However, so far, no x-ray system has been automated to make autonomous decisions (in order to satisfy FAA requirements for acceptable explosives detection systems), although several vendors are working on such modifications. In general, x-ray systems are under development by large- or mid-sized established commercial manufacturers and these systems are modifications of their current products. New x-ray systems can therefore be brought to the market much more rapidly than most of the other devices discussed earlier in this section.

The most important new developments in x-ray systems are in the areas of dual- or multi-energy systems, backscattered x rays, and computerized x-ray tomography (CT). Dual- or multi-energy systems are able to distinguish between low and high Z (or atomic number-the number of protons in a given nucleus) elements to a degree and can present the viewer with two or more images that emphasize the different materials (e.g., by color differentiation). Commercial devices with this capability are produced by EG&G Astrophysics and Siemens-Heimann.

A somewhat different approaches the Z-Technology (a trademark), or back-scatter x-ray system developed by American Science& Engineering (AS&E). In this case, the low Z image is created by a different process, i.e., detection of Compton backscatter radiation. Commercial Z-Scan systems exist and the manufacturer is now attempting to develop an automated pattern recognition approach that will meet the FAA's EDS requirements. Discrimination between high and low Z, although useful, does not specifically and uniquely identify explosives.

Another x-ray system under development is based on the application of medical computerized tomography (CT) technology to explosives detection. One company, Imatron, is close to having a prototype unit on the market able to produce three-dimensional images of suspicious items within a suitcase using CT processing. Through analysis of the data, they claim to be able to determine density to a high degree of precision. This provides a strong clue for detecting explosives. The demanding computing requirements of this system limit the speed at which it can operate, thus affecting throughput. All the above x-ray systems are discussed in appendix B.

Explosives Detection by Magnetic Resonance and Nuclear Quadruple Resonance

Bulk explosives may also be detected by magnetic resonance methods-both nuclear magnetic resonance (NMR) and electron spin resonance (ESR). The general technique is to place a sample in a uniform magnetic field and to expose it to a radio-frequency (RF) electromagnetic field. Then, the procedure requires varying the frequency (or the magnetic field strength) and noting the frequencies (or magnetic field strengths) at which the sample absorbs or emits RF energy.

The nuclear quadruple resonance (NQR) method employs a similar procedure but does not require a uniform magnetic field. It has been used to detect both non-nitrogenous and nitrogenous explosives in the laboratory.

The feasibility of detecting bulk explosives by NMR, ESR, and NQR in operational contexts has been studied for several years in the United States and the United Kingdom. For detecting sheet explosives containing nitrogen or chlorine, NQR appears especially promising. The final report of this assessment will discuss in greater detail the detection of bulk explosives by these three techniques.

Vapor Detection by Chemical Means

Man-made vapor detectors must perform three general steps. First, a sufficiently large sample of molecules must be collected. Second, interfering materials and impurities must be removed, the sample must be concentrated, or both. Finally, the remaining material must be tested in a way that will respond uniquely to the presence of explosive compounds.

The extremely low vapor pressure of many of the materials listed in table 4-1 makes the first step--collection of an adequately large sample of molecules-a serious challenge (see figure 4-5). EGDN has the highest vapor pressure among the common explosives and will be present in a saturated volume of room temperature air at the relatively high concentration of 1 part per 10,000. Chemically, EGDN is similar to the antifreeze commonly used in automobiles, differing only in that it contains two nitro ($-NO_2$) groups. Like its antifreeze cousin, bulk quantities of EGDN exposed to the air are rather easily detected even by that relatively insensitive detection device, the human nose.

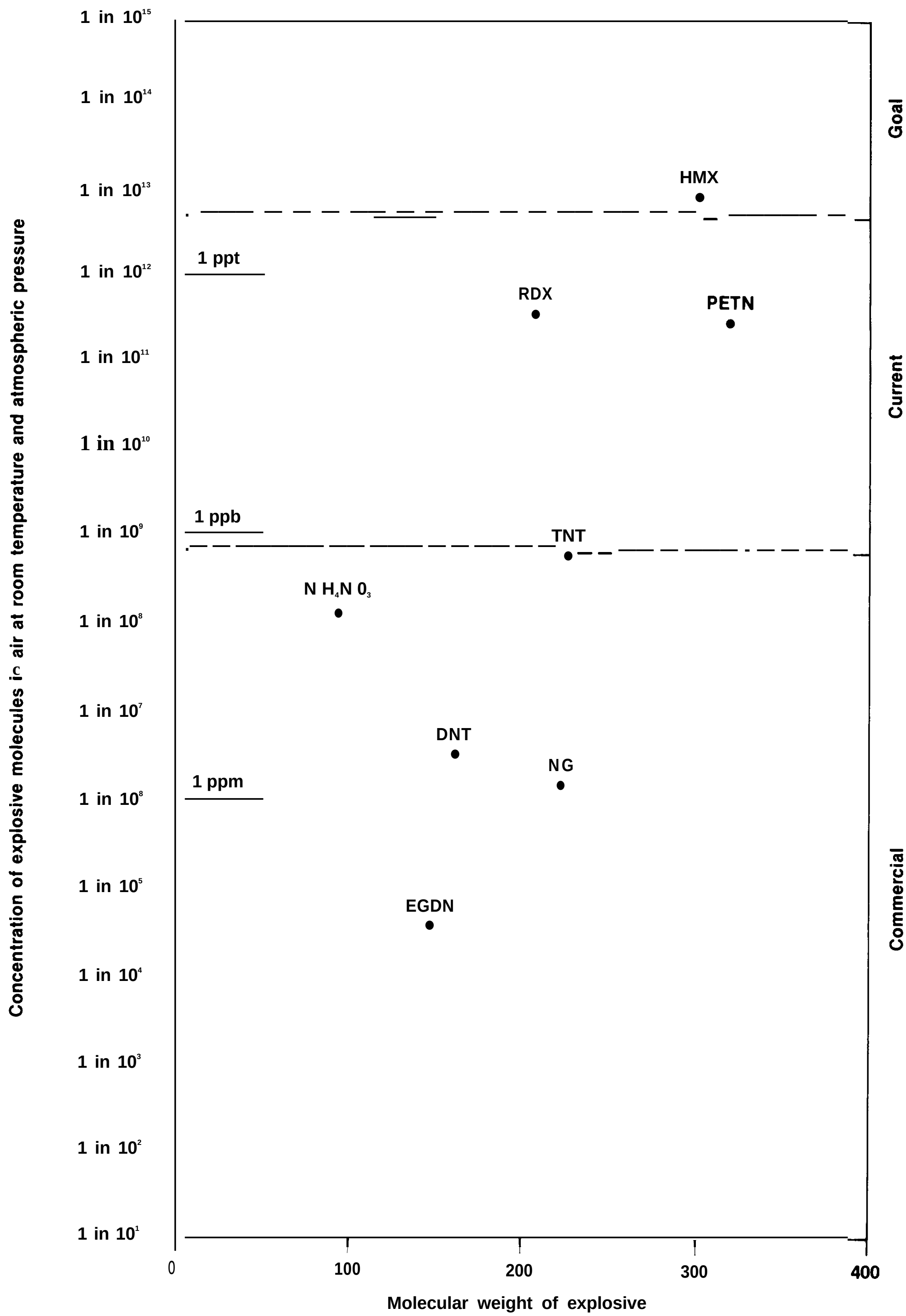
A saturated vapor of DNT (dinitrotoluene, a common contaminant in TNT--trinitrotoluene) or nitroglycerine (NG) will contain about one molecule of target compound per million molecules of diluent. Ammonium nitrate (AN) and TNT itself will be present at a concentration of about 1 part in 100 million (10^8). The plastic explosives RDX and PETN are even less volatile, being present in a saturated volume of air at standard temperature and pressure at a concentration of one part in one million million (or trillion—10^{12}). This concentration is comparable to one shot glass of whiskey in Loch Ness, about 30 cents out of the national debt or 1 second out of 32,000 years.[12] HMX is, by a factor of about 60, even less volatile. These concentrations represent saturation, a condition unlikely to be encountered in the field. Thus, in all likelihood, substantially less material than suggested here will be available for capture.

In addition to the vapor pressure of the pure compound, several factors affect the concentration of detectable vapor in the vicinity of an explosive. If an explosive device is contained within a more or less enclosed small. volume, after an extended time (on the order of hours or days) the concentration of explosive molecules within the enclosed space will build up towards equilibrium conditions. Air from such a suitcase or drawer or other container would contain near the maximum possible number of molecules. If the nearly saturated air could then be released and sampled, the probability of detection would be enhanced.

Another factor is the presence or absence of relatively higher vapor pressure contaminants, which are often introduced or created during the manufacturing process. While in many cases these contaminants have not even been identified, they nevertheless will cause some of the detectors to alarm. The concentration of these contaminants in the air surrounding a sample of explosive is a function of their concentration on the surface of the piece. Thus, they are most easily detected around a freshly broken piece. As they evaporate from the surface, their concentration near the explosive's surface declines. Molecules of the contaminant will, over time, diffuse to the surface from within the bulk

[12] Courtesy of Frank Conrad, Sandia National Laboratory.

Figure 4-5-Relative Volatilities of Some Common Explosives



SOURCE: Sandia National Laboratories, 1990.

of the explosive but this is a relatively slow process. Therefore, while such contaminants can be a benefit to the detection process, their presence cannot be relied on.

Finally, the presence or absence of physical carriers will have a profound effect on the motility of explosives molecules. Many researchers now suspect that most sniffers are not responding to molecules of the explosive compound in the pure vapor state, but rather to molecules attached to small carriers such as dust specks.

The relatively high electronegativity of these explosive compounds is a mixed blessing. It causes the molecules to be "sticky," rather in the way that static electricity makes balloons cling to a wall. This electronegativity is helpful for detection in that it makes the explosive compounds rather unique among organic molecules in their ability to attract and retain electrons, thereby forming negatively charged species (anions). The formation of anions is used by several detection schemes in testing for the presence of explosive in a sample. But this same property also causes difficulties for detection because the molecules bind to surfaces so strongly that shaking them loose in order to sweep them into a detector is not easy. Further, this affinity of the molecules for surfaces further depletes their concentration in the air sample. These twin effects form both the basis and the bane of many devices used to increase the concentration and number of molecules at the detector part of a sniffer.

The first stage of a sniffer will usually sample the incoming air by drawing it over a surface onto which the sticky explosive molecules attach themselves. In this manner, the molecules contained in a large volume of air maybe captured. Later, on heating the surface, the molecules are driven off. By performing this heating step in a stream of gas of much smaller volume than the originally sampled air stream, the concentration of the explosive molecules is enhanced. Unfortunately, not all (or even most) of the molecules are actually shaken loose from the adsorptive surface by the heating step. Thus, while the resulting stream contains a greater *concentration* of explosive molecules, there is, nevertheless, a decrease in the *absolute number* of molecules available for detection.

The thermal instability of these compounds is a problem because the same aggressive efforts @eating) sometimes needed to separate a sample of the explosive from a substrate, so that it may be channeled to a detector, can also cause the compound to degrade into smaller fragments that go unrecognized by the detection equipment.

On the other hand, some detection techniques actually depend on a related property, the frangibility (fragmentation) of these compounds. On impact with the proper targets (70 eV electrons or atoms of an inert gas, for example), these molecules will fragment. Under the right conditions, the kind and number of fragments into which the explosive molecules break down is predictable. In this manner, the presence of an explosive compound in the tested vapor may be confirmed. The two-stage mass-spectroscopy device described in appendix C takes advantage of this property.

The capture of a sufficiently large number of molecules of the explosive compounds probably constitutes the most difficult step for the sniffers. The explosive compounds do not shed many molecules into the air on account of their low volatility, and, consequently, successful vapor detectors must be sensitive to the presence of pico- or even femtogram quantities of material (10^{-12} and 10^{-15} gram respectively). The performance of vapor detectors can also be degraded by the presence of interfering materials and impurities, which can both trigger false alarms and lower the sensitivity of the equipment to real explosives. Finally, the effectiveness of the system is dependent on matching the detection strategy to the properties of the specific explosive compound present.

In the United States, until very recently, tests conducted on sniffers did not yield very favorable results. In March 1988, the FBI examined the performance of four commercially available explosives vapor detectors under realistic conditions. While most of the instruments could easily and reliably detect pure samples of the higher vapor pressure materials (EGDN and NG) under laboratory conditions, results in real world scenarios, including searches of suitcases and cars, were disappointing. The authors concluded:

[13] 'Explosive Detector Evaluation%' FBI Laboratory, Forensic Science Research amd Training Center, FBI Academy, Mar. 21-24, 1988, p. 65. A limited distribution report. Registered copies forofficial use are available by writing on letterhead to the FBI Academy, Quant.ice, VA 22135.

> [T]he challenge still remains to find a small hand-held detector able to reliably detect inorganic and plastic-based explosives in operational scenarios.[13]

In tests conducted by the FAA in 1989, another kind of sniffer, a chemiluminescent device (see app. C), also did not perform well. Results of this test have not been published. On the other hand, several foreign countries have found considerable promise in more advanced chemiluminescent units recently tested in a number of applications, including some baggage screening for airline security. In late 1990, the FAA ran tests on several vapor detection devices. The results of these tests have not yet been made public.

Vapor detection schemes do have certain advantages. They seem to be more amenable to automation because the typical output of the machine is a fairly simple electronic signal that can be satisfactorily interpreted by a microprocessor. No complicated pattern recognition is involved. Further, by generally avoiding the use of large radioactive sources and their attendant public relations problems, shipping and exporting these machines is a simpler matter. For the same reason, unlike detectors using large amounts of ionizing radiation, they can be used to screen radiation-sensitive subjects, such as humans. Also, because they generally do not require any shielding, they can be smaller and more portable and thereby more versatile than bulk detectors. For example, they are available as hand-held units that can be carried around a test object by a single person. They are much cheaper, usually by a factor of 10 and sometimes even by a factor of 50 or more, than nuclear-based devices. Finally, techniques are being developed to compensate for the low volatility of the explosive compounds. For example, some experts have had success using a swab to wipe down a suspected person or object, then testing the swab for residues. These detectors are being used in a variety of search scenarios.

A discussion of some of the different techniques and devices under development for explosives vapor detection may be found in appendix C.

Taggants

Given the difficulties in detecting small but deadly amounts of explosives, either by vapor detection or nuclear techniques, alternative possibilities need to be explored. A suggestion to this end, which has been discussed for years, is to place some agent in the explosive during manufacture that would make detection far easier. In the past, the principal goal of tagging explosives was for forensic purposes, that is, to try to aid in discovering the manufacturing origin and procurement path of an exploded bomb by careful examination of the residues of the explosive at the scene. Many possibilities were suggested and analyzed in an OTA report in 1980.[14] Suggestions for incorporating taggants in explosives were strongly opposed by manufacturers and by the National Rifle Association for several cited reasons: unacceptable added cost, complication to the manufacturing process, reduced performance (particularly of ammunition), and lack of effectiveness for detection, since foreign or clandestine manufacturers would not use the taggants.

However, in response to recent terrorist attacks on civil aviation, there has been a renewal of international interest in adding taggants to explosives. The International Civil Aviation Organization (ICAO) has organized a technical group to study this matter, and research is centering on a small number of possible chemical additives. Of particular interest is the fact that former Eastern bloc countries, including Czechoslovakia, have expressed strong interest in cooperating in this endeavor, doing so even prior to the recent accession of President Havel and a noncommunist government. The cooperation of Czechoslovakia would be particularly valuable because it is the manufacturer of SEMTEX, a favorite plastic explosive of Middle Eastern terrorists that was apparently used in the downing of Pan Am 103. Further, Czechoslovakia and the United Kingdom have cooperated in a joint United Nations effort to develop an international agreement on tagging. The likelihood of an international convention that mandates the inclusion of a chemical taggant during manufacture of all plastic and sheet explosives appears far more promising than it did some years ago.

---

13 "Explosive Detector Evaluation," FBI Laboratory, Forensic Science Research and Training Center, FBI Academy, Mar. 21-24, 1988, p. 65. A limited distribution report. Registered copies for official use are available by writing on letterhead to the FBI Academy, Quantico, VA 22135.

14 U.S. Congress, Office of Technology Assessment, *Taggants in Explosives*, OTA-ISC-116 (Springfield, VA: National Technical Information Service, 1980).

The principle of a chemical taggant is to introduce into all manufactured explosives a particular type of molecule that is easily detectable by vapor detectors. There are several requirements for such a taggant. It must be cheap and usable in small amounts, not unduly complicate the manufacturing process, and be easily available, nontoxic, safe, and easily detectable. A multinational working group is investigating several compounds. All are explosives themselves with relatively high vapor pressures, which would aid detection with sniffers. Other compounds are also being investigated. The feeling among the participating officials is that the international group may agree on a single compound in the near future. Efforts would then be made to arrive at an international manufacturing convention.

The only United States participation in tagging research is being carried out under a small contract with the U.S. Army Armament Development Command at Picatinny Arsenal in New Jersey (about $35,000 in fiscal year 1989 and a like amount in fiscal year 1990) with funding provided by the TSWG.

Another approach, pursued only on a theoretical level thus far, has been suggested. The concept considers the possibility of doping all explosives during manufacture with a minute amount of a radioactive isotope. Taggant concentrations as low as 10^{-12} grams per kilogram of explosive should allow one to detect a signal above ambient, natural radioactive background. Passengers and baggage would be screened by detectors that look for the characteristic radioactive emission at entry-ways in airports, similarly to current practice with x rays for carry-on baggage and with metal detectors for passengers. Unlike the chemical additives case, detection would not rely on the presence of vapor. Attempts by a terrorist to shield the gamma rays would be detected because of the large amount of heavy metal required.

The radioactive content of a bomb composed of the doped explosive would be less than that in a human body. Consequently, health hazards would be essentially zero. Many more orders of magnitude of radioactive exposure would be received by an airline crew and passengers from exposure to the natural background during a flight than by being surrounded for hours by explosives doped with this taggant.

One problem with this latter approach is the potential public opposition to anything radioactive, even if the quantities involved were so small that exposure to a passenger carrying the explosive on his body would be much lower than he would receive, for example, from sitting next to another person (industrial exposures would also be insignificant). Measurements in support of this concept have yet to be made. If background levels turn out to be higher than anticipated in an operational airport situation, more of the taggant might be needed (although the concentrations would still be far less than should occasion any health concerns).

However, there are two serious problems with tagging of any kind. The first is the large amount of explosives already in the hands of terrorists and their state sponsors.[15] It would take years, perhaps 5 to 10 or more, before this material would become unreliable. Nevertheless, one can argue that one should start at some time to tag explosives, because eventually the material in the current world inventory will run out.

But there is a more difficult objection, **namely that some terrorist groups now have the ability, possibly as individual groups or else through contacts with their state sponsors, to make their own plastic high explosives. These** illegitimate manufacturers will, of course, not tag their explosives, and no international accord could guarantee that they would. **Therefore, tagging would only raise serious difficulties for terrorists who have no access to illegitimate, nontagged sources and, even for them, probably not until some years in the future.**

DEFENSE AGAINST CHEMICAL AND BIOLOGICAL WARFARE (CBW) AGENTS

Although few overt and no major events have yet taken place, there is a consensus that a chemical or biological (CB) terrorist threat exists. A brief discussion of the threat was given in chapter 3. The level of technological sophistication required to mount a terrorist attack of this type is not particularly

[15] See, for example, The Washington *Post*, Mar. 23, 1990 for the report by President Havel of Czechoslovakia% who announced that the previous regime had sold 1,000 tonnes of SEMTEX to Libya and further amounts to other terrorist-sponsoring states, such as North Korea, Syria, Iran, and Iraq.

high. In fact, for some scenarios, it may be lower than was the case for some of the sophisticated bombs that have been used against civilian aircraft. Further, the ability of Libya, Iraq, and Iran to produce chemical weapons has been known from open sources for some time, and all of these countries have sponsored active terrorist groups that have attacked civilian populations with the aim of producing many deaths.

However, in the absence of actual examples of terrorist attacks employing chemical or biological agents, it is extremely difficult to substantiate or even define the threat accurately. In lieu of concrete evidence, and armed with some intelligence data, planners have found it necessary to look to U.S. military programs (which are, however, designed for battlefield applications) as a guide for devising responses to such events.

Research and development into the problem of detecting CB agents, either on the battlefield or in a terrorist situation, is not very advanced. Detection of biological agents and subsequent (or, frequently, concurrent) diagnosis of the agent causing the symptoms is relatively undeveloped. As a point of reference (that is, admittedly, 15 years old), in 1976, it took the full resources of the U.S. Government 7 months to isolate the Legionnaires' disease *Legionella pneumophila* bacterium when it was discovered.[16] [17]

The U.S. Army has primary responsibility for detection of chemical and biological agents. It has a modest research program and a few field detector systems under current development. The Army also maintains related intelligence activities that continually assess the chemical and biological threat, including the likelihood of their use by terrorists.

Biological agents are powerful; very small quantities can produce serious and widespread injury. They may be divided into three classes: those that infect those immediately exposed, but do not easily contaminate others who come into contact with the victims; those that are highly contagious and may cause epidemics; and those that are not living organisms or viruses, but are chemicals produced by organisms and only affect those exposed to them. An example of the first type is anthrax; the second type may be exemplified by ***Yersinia pestis, the*** bacteria that causes plague; the third type is comprised of toxins, such as botulinum toxin.

Table 4-4 gives some typical detection goals set by the U.S. Army for several of the most common chemical and biological agents envisioned as possible threats. The quantities cited give an idea of their effectiveness. United Nations experts have estimated that a person drinking 100 milliliters (less than a half cup) of untreated water from a 5 million liter reservoir would become severely sick and perhaps die if the reservoir had been contaminated by 1/z kg of Salmonella typhi (the causative Organism of typhoid fever), 5 kg of botulinum toxin (a plausible toxin warfare agent), or 7 kg of staphylococcal toxin (another plausible warfare toxin). By contrast, it would require 10 tons of potassium cyanide (a chemical warfare agent) to contaminate the reservoir to the same toxicity.

Chemical and Biological Agents—Point and Remote Detection

Preparation for such an ill-defined, amorphous threat is obviously a problem. Very little work directly aimed at the terrorist threat has been done; more research has been aimed at the battlefield threat. However, some of the detection research being conducted by the Army for its chemical and biological warfare defense program has direct applications to counterterrorism. There is also some research specifically directed at CBW counterterrorism that is being conducted at the Army Chemical Research, Development and Engineering Center.

The battlefield situation differs from the terrorist situation in some aspects. In the battlefield, airborne agents would be the main, although not the only concern. The role of technology is aimed at first, early detection to permit doming of protective gear; second, assessment of potentially contaminated areas to determine if, indeed, there is contamination, and, if so, what kind there is; and third, decontamination of contaminated areas.

In the terrorist case, large concentrations of people or high-profile fixed facilities (e.g., embassies) could be targeted. Also, agents might be placed in water supplies as well as transmitted through the

[16]Retrospectively, researchers have established that this microorganism did cause recorded disease as early as 1943.

[17]There is recent evidence that capabilities are significantly improved: the Army recently rapidly identified a strain of Ebola virus in a colony of monkeys to be used for medical research in Reston, VA.

Table 4-4-Chemical and Biological Agent Detection Goals

Chemical agents	Detection goals in air
GB (Sarin)	0.05 mg/m^3
GD (Soman)	0.05 mg/m^3
VX	0.002 mg/m^3
HD (a Mustard Gas)	5.0 mg/m^3
L (Lewisite)	5.0 mg/m^3

Biological agents	Detection goals
T-2 Toxin	2.0 mg/m^3
SEB (Staphylococcus Enterotoxin B)	0.01 mg/m^3
Botulinum Toxin	0.0007 mg/m^3
Yersinia Pestis	6×10^4 organisms/m^3
Coxiella Burnetii	6×10^4 organisms/m^3
Rift Valley Fever Virus	6×10^4 organisms/m^3

SOURCE: U.S. Army, 1990.

air in aerosol form. Early detection is of importance, but to allow timely evacuation to safe locations, not (unless the targeted population has been prepared and is in a high state of alert) for donning protective clothing or masks. Further, large areas may have to be monitored for long periods of time. For monitoring airborne agents, this would demand long-range, automated detectors with low maintenance problems for adequate early warning protection. The requirements for assessment and decontamination after an attack would demand similar technologies to the battlefield case. However, in the terrorist case, time scales for action would be longer than in the battlefield. Moreover, the areas to be covered might be much larger.

There are three generic types of systems under investigation for detecting CB agents: point detectors for early but relatively unspecific warning in the field, assay systems for specific identification of the agents involved but not necessarily intended for field use, and stand-off detectors that can monitor clouds-of chemicals or, perhaps, biological agents, from some distance. In contrast to explosives detection for airline security, there is no well-defined requirement that mandates exactly how detection systems might be used. Much of the current research is aimed primarily at producing detection or assay capability that could be available in Army field situations and in selected special locations, such as U.S. Army chemical and biological warfare laboratories or Public Health Service laboratories. Beyond detection systems, there is some portable protection equipment being developed for emergency use in special highly critical situations.

A major difficulty in the detection of a chemical or biological attack is the variety of possible agents and the need to search for (often specific) known agent signatures. This immediately limits the detection process to those substances known to the defender. A new, previously unknown substance might well go undetected, at least for a while. Unfortunately, there are no general characteristics of agents that one can look for. Point detection systems are generally based on introduction of antibodies for the specific agents, and the subsequent detection of the antibody/antigen reaction or resulting compound. The detection goals vary with the agent, as seen in table 4-4, depending on human sensitivity levels. Generally, these goals are set at less than a milligram per cubic meter, with chemical agents requiring fractional milligram sensitivity and biological agents usually requiring higher levels, but with great variety. The declared battlefield requirement for detection of botulinum toxin, for instance, demands the ability to find quantities as low as 0.0007 mg/m^3. Instruments usually consist of a sample acquisition system (e.g., a vacuum cleaner), a sample preparation step where the antigen is introduced, and a sensor system, which is supported by computing equipment that displays the result or provides an alarm.

For stand-off (remote) detection, most concepts employ passive optical and laser technologies. This field has benefited from research performed in the related field of environmental and atmospheric monitoring. Optical and laser radar technologies are also under development for a wide variety of other applications, including various Department of Defense missions. The search for counterterrorist technology in this domain often involves applications or adaptation of technological developments from other fields.

Stand-off detection equipment should be small enough to be mounted on a mobile platform, such as a van or helicopter (although there are also some freed site applications for guarding a point site or perimeter). The goal is to observe an area with a radius (stand-off distance) usually on the order of 1 to 10 km. Presumably, this range would give the intended victims enough warning time to react and try to protect themselves. The instrument should be able to scan the critical area, detect the presence of a cloud of dangerous vapor, determine its location, and discern its critical agents. Some of the optical and laser systems are also called onto detect ground contamination. Both stand-off detectors and point detectors need to know just what agents to look for. For remote optical detection, the emission or absorption spectrum of the agent must be known in advance.

Appendix D provides a discussion of research projects aimed at developing detection of or protection against terrorist attacks using chemical and biological agents.

PHYSICAL PROTECTION

In this section, and for the rest of the chapter, the bulk of the discussion will be generic rather than specific. However, a few illustrative projects will be discussed in order to give a flavor of interesting avenues of research that may be appropriate and promising.

Rather than provide a compendium of detailed barrier information, this section describes briefly a number of well-known, available technologies, and refers to some documentation for further information. Development efforts in this area are usually engineering refinements rather than efforts to develop radically new technologies or techniques.

Physical protection encompasses a wide variety of technologies that have been aggressively developed for several decades. First, the military has long had an interest in providing physical protection for its bases and facilities, at home and abroad, during war and peace. Further, since the advent of nuclear weapons, the Atomic Energy Commission and its successor agencies, most recently the Department of Energy, have devoted considerable effort to the vital task of protecting and maintaining control of nuclear weapons and the special nuclear material (enriched uranium and plutonium) that fuels them. Both the Department of Energy and the Department of Defense have active research programs to improve levels of physical protection around both freed and mobile sites. The Nuclear Regulatory Commission oversees an active program of protection of civilian nuclear facilities, including specific regulatory standards for such equipment. Finally, private corporations, often being the targets of terrorist attacks, have pursued physical security for many years, resulting in a thriving industry that furnishes protective devices for their needs.

Much of the purely military effort takes place at Fort Belvoir, at its Research, Engineering, and Development Center; most of the physical protection research for the nation's nuclear weapons complex is directed by Sandia National Laboratory. Also, considerable efforts are funded by the Defense Nuclear Agency. Many of the technologies (e.g., advanced barriers, perimeter detection systems, alarms) that have been developed by these agencies are applicable in a number of counterterrorist contexts.

In the counterterrorist context, physical protection is a function of likely target type. There are domestic freed sites, such as government buildings, military bases, and airports; there are overseas sites, such as embassies and, again, military bases. Buildings belonging to private U.S. corporations, both in the United States and abroad, may also be targets, as might gathering places for U.S. citizens, such as particular bars or theaters. Plants associated with the nuclear weapons complex are an obvious target for nuclear terrorism. Mobile targets may be military, but they may also be civilian aircraft. It is of interest to investigate whether one might harden aircraft against internal explosions, or protect them against missiles while in flight.

Concerning airline security, there currently are programs to design security systems for airports that would make both hijacking and sabotage more difficult. In this field, lessons learned in designing security systems for other facilities, such as plants in the U.S. nuclear weapons complex, may prove useful in assembling integrated systems for airports. Of course, changes must be made in system details, but design methods and many individual technologies (e.g., weapons and explosives detectors) employed in the nuclear security effort maybe of use. A key question, however, is the eventual cost of such systems.

Sandia National Laboratory has been given the role of lead laboratory for research and development in physical security for the Department of Energy. For several decades, it has performed work in developing, testing, and evaluating barriers, sensors, alarm systems, and delaying techniques.[18] Many component technologies are already commercially available. Originally aimed at developing the best possible protection for nuclear weapons, whether

[18] For further and detailed discussion of man, sensor and barrier technologies, see Sandia National Laboratory, SAND87-1924 to SAND87-1929, July 1989.

under transport or at fixed sites, whether in the United States or abroad, Sandia's mandate has more recently extended to assisting other agencies, such as the Department of State, the Secret Service, and the Bureau of Engraving and Printing. Safeguards engineering research at Sandia, under which aegis most nuclear weapons protection work is done, is funded at about $60 million for fiscal year 1990. Most of this work is not oriented towards counter-terrorism, but the results may often be useful for this purpose.

The principle invoked in designing security systems for many physical protection problems is to divide the defense's task into three parts: detection, delay, and response. The first part deals with detecting an intrusion or an attack by a malefactor, and, impossible, identifying and assessing the nature of the intrusion. The second part covers barriers of diverse sorts that are either in place or can be deployed rapidly (within seconds) to respond to the intrusion. The last of these three parts refers to the arrival of a military or police force to respond effectively to an attack. Detailed discussion of this topic is beyond the scope of the present study, although mention of technologies for assisting specific response scenarios is made in the following sections. Technologies for carrying out the first two tasks are of interest here. Most of these technologies are well developed. The task of systems designers is to integrate the parts into an operationally useful and economically affordable system. In the area of nuclear terrorism, this has been done, although upgrades are continuing.

Detectors and Alarms

Detection may be accomplished by many methods, most of which are commercially available for domestic or commercial security systems. Alarms and detectors may be deployed along a perimeter around a site or in isolated rooms that are normally unoccupied. Microwave sensors emit microwave radiation and operate either by observing the blocking of a beam by an intruder (bistatic mode, with a separate transmitter and receiver) or by receiving the reflected radiation of a transmitted beam from an intruder by means of a receiver that is collocated with the transmitter. Similar techniques can be used at wavelengths shorter than radar, namely in the infrared regime. Also, since most living objects of interest are warm (about 310 K), they emit infrared radiation at wavelengths between about 10 and 30 micrometers. Passive infrared detectors use this fact to detect living objects in a protected zone. Passive infrared detectors are being developed by the Defense Nuclear Agency and the U.S. Army as well as by Sandia for specific military needs. Other types of detectors, seismic sensors, pick up the small vibrations generated when a human or animal is simply walking nearby. Still others detect variations in electrical fields when a passing intruder's body changes the average dielectric constant in his vicinity. One potential application of alarm technology would be to place sensors around unattended commercial aircraft so that persons attempting unauthorized access would be detected and, if possible, identified.

Each of these techniques can, in principle, be defeated by a variety of countermeasures. A cleverly designed security system makes use of several techniques together so that countering all of them becomes an extremely cumbersome and complicated task for a would-be terrorist. Another consideration in designing a system, particularly one for outdoor use, is to employ methods and combinations of technologies to prevent stray animals, wind, or naturally occurring events from triggering alarms. No system is useful when the false-alarm rate is high.

Another useful detector is the closed-circuit TV camera. Sophisticated electronic and software additions have been developed that can make a mundane security system far more effective. By comparing, for example, a current image with an earlier one, scene changes may be highlighted or, by using clever algorithms, the system may trigger an alarm when scene changes corresponding to a serious threat occur. The software may detect changes from scene to scene (perhaps only seconds apart in time) that indicate a human- or vehicle-sized object moving toward a protected zone at a rate consistent with the expected speed of an intruder.

Barriers

Barriers may range from simple high fences (not a very good delaying technique for a determined adversary) to very thick reinforced concrete walls. Barriers may be alarmed as well. Barrier design is chosen to be applicable to the specific site. A mobile military site may have a simple fence and rely on distant perimeter alarms to protect a central zone. An embassy may have stand-off barriers, such as high fences or walls that are difficult to scale. One may emplace high berms (to deflect pressure waves from a blast and to block shrapnel) and vehicle barriers scores of meters from the defended site to help protect against car bombs. Very sensitive items, such as nuclear weapons, maybe protected in a vault shielded by reinforced concrete.

Delaying techniques have been developed by Sandia for use inside buildings. The range of technologies is diverse and impressive, not always relying on radically new, high technology engineering. These may run from smoke- and liquid-foam generating devices that can effectively impede and slow down intruders to coils of razor wire that may be dropped from a ceiling to fill a room.

Building Hardening

Architectural design and mechanical engineering are two disciplines of particular use to the State Department and would be of use to any entity wishing to protect its buildings against catastrophic collapse induced by explosions. One may design or (less desirably) retrofit buildings to make them more resistant to explosions, either nearby or within. Following the attacks on U.S. Embassies in Beirut and Kuwait in the early 1980s, the State Department instituted a program to spend several billion dollars on improving security and blast resistance at its overseas sites. Features that should be avoided include unreinforced masonry, wood frames, cantilevered elements, and heavy concrete buildings supported by thin columns. In general, low buildings with closely spaced ties above and below floor slabs and with relatively short unsupported spans are more resistant. Many engineering practices useful in earthquake-resistant design are also applicable in defending against explosions. There is little that is new here, but there is a challenge in designing buildings that are esthetically pleasing, that retain an openness that the United States wishes to maintain in its public buildings, and that still provide some protection against serious sabotage. Modifying existing structures to have such features is more difficult and expensive than incorporating them from the beginning.

Aircraft Hardening

An area receiving new interest is the possibility of hardening parts of aircraft to prevent, impede, or mitigate terrorist acts. If appropriate lightweight armor could be found that would, for example, protect the flight deck from gunfire, this would be helpful in controlling attacks on the crew. Such attacks are infrequent, but do occur, as in the case of a PSA flight in 1987, when a disgruntled ex-employee shot the crew and caused the aircraft to crash, killing all aboard. Areas that might be protected could include crew seats, the bulkhead separating cabin from flight deck, and the cabin door.

Another promising topic being investigated is whether baggage containers could be constructed of lightweight, protective material that could partially contain an explosion, venting it in a semi-controlled manner. Possibly, blow-out panels could be built into aircraft fuselages at positions corresponding to venting points of the containers. These might prevent propagation of holes or tears in the aircraft skin that could lead to catastrophic failure. Thus, the integrity of an aircraft might be protected during flight. Of course, a large enough explosive would be able to breach any containment one might design, since the containment mass would have to be limited in an aircraft. However, if the required size of an explosive were driven up significantly, this would greatly facilitate the task of explosives detectors of all types in preventing such items from being brought on board.

As an example, one corporation, QSI, Inc., has developed a lightweight armor, designated QX-90, which is composed of laminates of various composites. Originally designed for body armor, and successful at stopping 7.62 mm armor-piercing ammunition in a $^{7}/_{32}$ inch layer, this product is being examined for such an application.

Further, the FAA Technical Center has a program to examine means of reducing and mitigating the vulnerability of aircraft to explosions in flight. These would appear to be useful lines of research to pursue, since payoff could be very high, and (at least initial) research costs in materials research would be relatively low. Our subsequent report will examine this topic further.

Access Control

Control of ingress to and egress from protected areas is a necessary part of physical security for many applications. In general, the facility's security plan requires individuals who wish to pass a secure portal to be screened for access. Usually, the individual will be an employee who requires access to the area in order to perform his or her job. Also, this process permits a control center to keep track of who is where in the facility by means of a continually updated database.

A potential area of utilization is airport protection. It is necessary to prevent unauthorized persons from gaining access to critical zones, for example, those in which aircraft are located. In busy airports, there are thousands of employees and hundreds or even thousands of portals. Airports are now required by the FAA to control access to air operation areas in order to prevent the entry of unauthorized persons and ground vehicles.[19] Practical implementation of this rule is currently underway. About half the Nation's major airports have submitted access control and airport security plans. Some difficulties have arisen: now that specific standards are being addressed and described, objections from airport operations authorities have developed, particularly regarding cost and operational questions.

The problem of maintaining adequate entry control is complex. A successful system requires sophisticated computer control and system design as well as devices that can automatically grant access to legitimate requesters. More sophisticated versions will add the ability to grant different levels of access to persons with different levels of authorization. Some areas might be accessible to all employees and other more protected areas to only a few.

The technology to support access control is well-developed and commercially available. The most common and simplest technique uses an identity card combined with a Personal Identification Number (PIN) for each authorized individual. However, direct measurements of unalterable characteristics of the individual provide surer identification. Among more advanced technologies are four of interest: voice pattern recognition, fingerprint examination, hand profile measurements (in which several dimensions of an individual's hand are automatically measured), and retinal pattern identification. One could also simply use a TV camera-a remotely located security officer could compare the image with a photograph. Automating this process is a technology that requires further work to achieve cost reductions.

The four more advanced identification technologies noted above have been evaluated by Sandia Laboratory and all were found practical. The quickest among the evaluated models was the hand profile monitor, which required less than 5 seconds for examination and had very low rates of false positives and false negatives (less than 1 percent).

An identification technique now in the early research stage examines the pattern of an individual's iris. This is done with a TV camera that is linked to a computer employing appropriate software algorithms. The iris pattern of an individual appears to be a highly specific identifier. A computer can be taught to recognize distinctive features of the iris in a TV image and then express them in a digital code, which is then stored in a computer or on an identification card. In possible border-control applications, irises of those seeking entry would be imaged by a TV camera, computer-coded, and matched by computer against the iris patterns of those (e.g., criminals or terrorists) on watch lists. A central problem in this application is obtaining detailed images of the irises of undesirables. In any case, many matches may have to be attempted before one is found, so the matching algorithms and the computer need to be fast.

In a more typical access-control application, irises of those seeking entry may be matched against the irises of those authorized access.

Baltimore-Washington International (BWI) Airport Project

Sandia National Laboratory is conducting a study, funded by the FAA Technical Center, to investigate how security might be upgraded at typical airports. This multiyear project, called the Enhanced Security Demonstration Project, is underway, using Piers A and B at Baltimore-Washington International Airport as a test-bed. Sandia is applying to airport security those design techniques developed over decades for protecting nuclear installations. Much of the planning is done by experts who have been working on physical security for years. But the effort also uses computer programs to model the physical security system of the airport in an effort to find and close paths that malefactor might use for hijacking or sabotage.

Currently, airports can defend themselves well against one or a few disorganized hijackers. The goal of the project is to design an airport security system

[19] 14 CFR 107.13, FAA Regulations.

292-884 0 - 91 -- 3 : QL 3

that would protect the airport and aircraft against an organized group attempting to hijack or sabotage aircraft, including the case in which there is an ‘‘insider’ with access to restricted areas of the airport who colludes with the terrorists.

One technique is the use of a computer model developed by Sandia National Laboratories, called ASSESS, that tries to discern all paths by which terrorists might introduce weapons or bombs aboard aircraft. The number of paths increases geometrically with the number of portals or potential points of access that one must defend. If one includes the case of colluding insiders, the situation becomes that much more complex. A computer can use its enormous calculating power to find subtle vulnerabilities not always apparent to human security experts.

The Sandia project is studying all aspects of security upgrading, from selection of optimal explosives and metal detectors to means such as installation of one-way revolving doors at passenger concourses to ensure that all individuals pass portals only in the authorized direction. Other concerns are the installation of optimally placed closed-circuit TV cameras at portals, employee screening at employee access portals, and duress alarms at portals, so that security personnel may surreptitiously indicate to a command post that a serious problem has arisen. Close attention is being paid to the layout of the facility. If, for example, public parking lots are close to areas where aircraft are found, detectors and barriers should be installed to prevent someone from throwing a weapon or bomb over a fence to a waiting conspirator with immediate access to aircraft. In addition, human factors are being investigated. These include motivating security personnel, making their tasks easier, and monitoring their activities.[20]

Sandia intends to implement upgrades at Baltimore in the 1991 to 1992 timeframe that would protect against a sophisticated hijacker threat.[21] Following this, further upgrades will be aimed at preventing well-organized terrorists from introducing bombs aboard aircraft. It remains to be seen when this latter aspect of the project will be finished, and what capital costs would be required to upgrade the security system accordingly at a typical airport.

Efforts to develop similar systems to design security upgrades for airports are also being considered by private firms. For example, Ameritec of Alexandria, VA is trying to adapt techniques they have developed for designing protective systems for embassies and other fixed sites. Another firm, Aerospace Services International, of Herndon, VA, is actively engaged in the design of security upgrades at Dunes International Airport and in the design of security systems at the new Denver airport.

INCIDENT RESPONSE

This section deals with technologies that could be used to deal with terrorist actions that last for a significant length of time rather than occurring essentially instantaneously (e.g., an explosion aboard an aircraft or a car bombing). The type of incident that is of interest is a hostage holding situation on an aircraft, in another vehicle, or at a freed site. There are at least two types of tools that would be of great potential use. One would be a detector that would allow authorities to monitor what was going on inside an enclosed area in which hostages were held, so that an assault might be planned most effectively. In the aircraft case, it would be useful to know, for example, where the terrorists were located, especially at the moment of assault, how they were armed, or whether any hostages were injured.

Another useful device would be a less-than-lethal weapon that would allow authorities to disable terrorists during an assault while not permanently or seriously harming them or the hostages. A dose of an agent could be administered either through inhalation or through percutaneous (through the skin) penetration. Such a hypothetical agent could be introduced into a confined area where hostages are held to disable the terrorists but not harm the

[20] Recently, United Airlines installed “high-tech’ security systems at O’Hare International Airport in Chicago and Denver’s Stapleton International Airport. As well as employing the latest in x-ray luggage scanners, United has looked closely at improving personnel performance through management techniques. One example is the practice of rewarding positive performance by both monetary and professional means. Good performers are offered the possibility of employment directly with the airline instead of remaining as “rent-a-cops” with a contracting security agency. Another example is the open microphone at passenger entry points that permit supervisors to monitor conversations among the security personnel. Reportedly, since installation of the new system, the number of detected contraband items has significantly increased. A similar system has also recently been installed at Dunes Airport in Washington.

[21] That is, a well-organized group of hijackers with advanced technical knowledge, unlike the primitive threats faced in the United States in the 1970s.

hostages. The rescue team could then free the hostages without risking lives.

There are some difficulties with this scenario. For example, a terrorist might wire explosives to a "dead man's switch," which he or she would then hold. After being disabled, the terrorist would then let go and set off an explosion. This tactic has been used, but very infrequently. Another difficulty, more general and more serious in developing such agents, is that the average dose required to incapacitate might not be sufficiently less than the average fatal dose. The very young and very old, and those with serious cardiovascular or cardiopulmonary problems would then be particularly at risk. Nevertheless, one can imagine many scenarios in which it would be very useful to have the option of using such agents (e.g., after the elderly and infirm have been released), provided the ratio of incapacitating dose to lethal dose were high enough.

Many classes of incapacitating agents have been investigated in the past, from LSD and THC (the active ingredient in marijuana) to glycolates and tranquilizers, such as chlorpromazine. Some have been dropped because of safety questions (e.g., rapid depression of blood pressure or respiration rate) and others because of lack of predictability in effect (e.g., LSD). Ideally, one would wish an onset within a few seconds or, at most, a minute, with effects that last for many minutes or a few hours.

Tests on some candidate compositions have been carried out on animals, but not on humans. One problem is extrapolating effects from animals to man. Unfortunately, it appears that as one proceeds to examine effects on higher species, the ratio of fatal to incapacitating dose appears to drop. Ratios of hundreds or thousands (which one would like) in mice and rats drop to 10s in primates, and are estimated to be on the order of 10 or less in man. Work is continuing in this area, not directly under counterterrorist research, but having clear application thereto. Interest also comes from the National Institute of Justice, which is looking for incapacitating agents for law enforcement use in lieu of firearms.

DATA DISSEMINATION

Communication among law enforcement, intelligence, and military authorities, both domestically and internationally, is a vital part of counterterrorist actions. There are two broad kinds of communications that are of interest. One deals with information and databases on terrorists and terrorism, and the other concerns information on progress in research and development of new counterterrorist tools. The latter sort of communication has been greatly aided by the existence of the TSWG, although much information is still not rapidly transferred. For example, attempts to compose a database on R&D progress have not yet succeeded, in part due to lack of funding.

Improvements in some facets of counterterrorist communications can be achieved through technologies. For instance, data exchange may be improved through technical means, such as encrypted communications and satellite links. In general, these goals may be accomplished without developing radically new technologies; it is usually a matter of designing and engineering the solution to a well-defined communications problem.

However, since some impediments to information transfer are a result of classification of information, turf battles, and legal constraints (e.g., on intelligence information that might be shared among agencies with external jurisdiction and those with internal law enforcement responsibilities), improvements in these areas will usually require addressing policy issues.

There have been some efforts to improve communications among the agencies that have overlapping authority in the counterterrorist field. Members of cognizant interagency committees are supposed to keep each other abreast of their own agencies' information in the field. Among other things, the exchange of R&D information is meant to avoid unnecessary duplication of research efforts by the interagency group. OTA has not yet assessed the degree of coordination that this process achieves, and will report on this in the future.

Another example of interagency data exchange is the use of a "flash board" system, essentially an electronic bulletin board among Federal intelligence, military, and law enforcement agencies that allows time-urgent information to be exchanged on secure lines in near-real time.

One major technical effort in the data dissemination area about which OTA has so far received detailed information is a large computer software and networking effort intended to assemble, update, and correlate all known information on terrorist groups. One eventual goal is to achieve a rough predictive capability of terrorist attacks--obviously not a precise prediction of target, date, and time, but rather an ability to issue plausible alerts over periods when attacks might be expected. Another aim would be to attempt to assess the nature of a specific threat.

The fundamental concept is to arrange information by terrorist group. Information may come from intelligence sources or simply from an open source such as press reports. It may include items such as movements of group members, money transfers, movement of equipment, or group dynamics and politics. One important systems aspect is developing appropriate protocols and formatting to input the information in an efficient way.

The eventual goal would be to provide general warnings such as that a given group appears to be planning an action, with general ideas of the type of target one might anticipate as the object of attack, and a timeframe for maintaining an alert.

Chapter 5

Conclusions Regarding Current Research and Development Into Detection of Explosives

A large number of detection systems are currently being developed. In addition to SAIC (developers of the thermal neutron analysis [TNA] method), several vendors have produced prototypes that, they claim, can usefully detect small quantities of plastic explosives. Some of these use vapor detection and some use x-ray imaging techniques. Among the vendors making such claims are Barringer, Inc. (vapor), Ion Track Instruments (vapor), Thermedics, Inc. (vapor), AS&E (backscatter x-ray), and Imatron (x-ray, using computerized tomography). The x-ray and vapor systems are significantly smaller and cheaper than the current TNA device. Further, other companies, such as EG&G Astrophysics and Siemann-Heimann, have commercial x-ray systems available that they claim are useful for explosives detection at airports.

After reviewing the current state-of-the-art, OTA sees no evidence that any device, currently at the prototype stage, is capable by itself of ***reliably***[1] detecting small quantities of plastic explosives in checked baggage. There are many technologies, including TNA, that have limited capabilities; however, all have serious flaws. Table 5-1 provides a summary of the qualities of the principal types of detectors.

Since each device has serious weaknesses, the best solution for a security system would be a combination of different technologies, if this could be made economically and operationally feasible. This would exploit the advantages of each technique while compensating for its weaknesses. As a hypothetical example (not a definitive prescription), a first step in screening might sequentially employ vapor detection and x-ray imaging devices, which are smaller and less expensive than TNA. Those bags that produced alarms in both systems would go to TNA and computerized tomography for a further look. This would reduce the number of heavy, expensive detectors at each airport, and, if false-alarm rates in the frost step were low enough, the cost and operational feasibility could be practical.[2]

Greater attention should be paid to passenger screening, which could provide a filter that would greatly reduce the number of bags that the technical tools would have to examine. If, say, 90 percent of passengers could be eliminated as likely carriers of explosives through a combination of profiles, interviews, and matching of passengers with baggage, the number of bags that required inspection would be reduced by a factor of 10. This would reduce the requirements for the explosives detection equipment with regard to number, size, and speed of throughput. This "human factors"-oriented security approach is highly labor-intensive, but has been used in Israel and by El Al Airlines worldwide to provide security with a good measure of success.

Many have criticized the suggestion that this approach be applied to the United States, on the grounds that the size of El Al's operation is minute compared to U.S. traffic. However, it would be a mistake to conclude that none of these techniques and procedures can be adapted from the Israeli experience for application on U.S. carriers. Further, where machines are used to aid human decision-making, there may be economies of scale in the United States.[3]

[1]That is, With a high (at least 90 percent) detection probability and a low (at most 5 percent and preferably much less) false-alarm rate. A significantly lower detection probability may not be sufficient to deter attacks by terrorists who are willing to risk the arrest of several operatives in order to achieve one spectacular success. Regarding false-alarrnrates, at least one foreign country has found that intensive scrutiny of about 3 percent of checked baggage is feasible without introducing more than a 2-hour delay between check-in and departure. This implies that a false-alarm rate of this order may be acceptable, at least in some settings.

[2]If the first step had a false-alarm rate of, say, 2 percent, only 1 bag in 50 would have to be examined by the following step. Then, instead of requiring that each TNA machine handle a flow of 600 bags per hour, as is currently specified in the FAA rule, published in September 1989 (see below), it would only be necessary for it to handle 12 bags per hour. This would mean that the number of TNA devices needed at a large airport would be 1 or 2, rather than 10 to 20.

[3]Our final report will examine this issue further.

Table 5-l-Advantages and Disadvantages of Available (or nearly available) Explosives Detection Techniques

Type	Advantages	Disadvantages
Chemiluminescence	Cost; size; sees plastics; specificity (determines molecular compounds with low rate of misidentification).	Slow; needs vapor or residues.
Electron capture	Cost very low; size;, may see plastics.	Slow; no specificity; needs vapor or residues
Ion mobility	Cost; size; may see plastics.	Needs substantial development; needs vapor or residues.
TNA	Sees plastics; prototype exists and being tested in airports; automated. No vapor needed.	Large; expensive; sensitivity currently inadequate; false-alarm rates high.
X-ray, dual energy, or backscatter.	In commercial production; high spatial resolution; may see sheets or small quantities of explosives; does some discrimination on atomic number, but only roughly; cost and size relatively small; can see other weapons; vapor not an issue.	Not specific to explosives; sensitivity to small or thin quantities uncertain; not yet automated.
Computerized tomography	Very high 3-D spatial resolution, good for small quantities of explosives or other contraband; prototype exists. Vapor not an issue.	Only looks at density; not specific to explosives; slow; large; expensive.

SOURCE: Office of Technology Assessment, 1991.

TESTING AND EVALUATION

With a potential market that could reach hundreds of millions of dollars within the next few years, it is to be expected that there will be a multitude of conflicting and highly optimistic claims made on behalf of many different products. Consequently, a credible, objective, official evaluation and certification procedure is badly needed. For this function, the government may wish to turn to an independent agency or body that is widely respected for integrity, scientific and technical expertise, and neutrality.

An independent testing authority, *outside the Federal Aviation Administration (FAA), is* urgently needed to provide a neutral testing protocol and to carry out such evaluations. It would be useful, if not essential, if this were to be accomplished and potential devices certified before rules requiring massive and expensive purchases of equipment are established. The FAA is on record as welcoming the establishment of such a body.[4] Following criticism from public officials and the Victims of Pan Am 103 organization, the FAA has also recently constituted an independent advisory panel that is to provide outside recommendations on testing protocols. The TNA equipment should be retested using new protocols.

Establishment of an independent testing panel would help the FAA avoid future allegations of conflict of interest. Some observers have criticized the agency for a perceived lack of objectivity in the past. These accusations were based primarily on two facts. First, specific technologies have been funded by the FAA for several years, creating the possibility of institutional bias in favor of those approaches. Second, serious questions were raised about the procedures used in the San Francisco Airport and Los Angeles Airport testing of the TNA device.

One possible agency for testing is the National Institute of Science and Technology (NIST), formerly the National Bureau of Standards. Not having participated to any important degree in the development of explosives detectors (although it recently tested a number of vapor detectors for the National Institute of Justice), it has no perceived "axe to grind"; it has a well-deserved reputation for scientific and engineering competence, and has performed, as part of its mission, evaluations of a multitude of engineering and measuring devices. Another institution with much experience is Sandia National Laboratory, which has worked in this area for over a decade. However, Sandia might be handicapped by the fact that it has worked assiduously on a few technical approaches for a number of years, and thus may be perceived as having a stake in developing them at the expense of others. Another possibility, the National Research Council of the National Academy of Sciences (NAS), which has concluded a study of the problem of explosives detectors for the FAA, is a respected body with the required technical capability. However, the NAS is not interested in being a testing laboratory, and, indeed, is not setup to perform this sort of task.

[4] Testimony of Monte Belger before the President's Commission on Airline Security and Terrorism, Feb. 2, 1990.

Any of the above institutions, however, would be excellent choices to develop appropriate protocols for the testing and evaluation of explosives detection equipment. In fact, the FAA has contracted with the National Research Council to develop some testing protocols for nuclear-based explosives detection methods.

A further alternative would be to contract with other outside sources, such as academic institutions, military laboratories, or private laboratories, to write protocols and perform the testing. In all cases, it would be useful to establish an advisory board, consisting of technical experts from several government agencies (e.g., the FAA, the Departments of Defense, State, and Energy), academia, and, possibly, the private sector, to oversee the testing and evaluation process.

MANAGING RESEARCH

Cooperation

A few Federal agencies are funding the major share of research into detectors for explosives. These include, of course, the FAA, which, in addition to working on vapor detectors and TNA, is pursuing a number of advanced technologies, described elsewhere in this chapter and in appendixes A through C. As another example, the State Department is funding Thermedics' chemiluminescent technology for detection of explosives in packages. A small amount of other work is scattered among other agencies.

Several specific examples have persuaded OTA staff that coordination among the agencies, both regarding cooperation and exchange of information, is in need of improvement. In recent months there have been signs of better interagency communication, but more needs to be done.[5]

Time From Laboratory To Deployment

A major problem is the length of time needed to go from laboratory work to deployment in the field. Although many Americans would like to have immediately a set of new, devastatingly effective tools to fight terrorism, the reality is that the time required to research, develop, prototype, and, finally, to field a particular device is often considerable. It can frequently take as long as 10 years to bring a new, complex technology to the commercial market. The first 2 or 3 years are usually spent in research, making fundamental measurements to determine the feasibility of an idea. Another 2 years are typically required to demonstrate the feasibility of a process or equipment. Two more years are often needed to develop a prototype, and as much as another 2 to 3 years are frequently spent in so-called "beta test sites" where the engineered hardware is rigorously tested in a realistic environment.[6] These lengths of time are rough estimates and not absolute rules that apply to every case. However, they are consistent with the experience with TNA.

This process may be shortened somewhat, but rarely to less than 5 years. The developmental time depends on the urgency of the project, whether the initial research is funded sufficiently to allow concurrent approaches to solutions of problems, the complexity of the hardware, and, most of all, the relation of the hardware to other existing, preferably commercial, equipment.

The time to produce a prototype can be reduced in the case where only a minor rnodification of existing commercial hardware, rather than a brand new class, is required. Modifications of existing commercial x-ray scanners fall into this category. Another major advantage of modifying existing hardware is that the manufacturing capability is likely to exist already.

To maximize the likelihood of success, long-term research often must incorporate different avenues of approach. In some cases, it may be advisable to back different groups working on similar technologies. Much basic research is a high-risk, high-payoff procedure. Coupling high-risk research with small studies that evaluate how a particular technical approach would fit into an integrated security system would be a useful approach in guiding long-range funding decisions and in determining which technologies to support. One especially important topic to study would be the definition of requirements for an integrated system, as opposed to requirements for component devices.

The FAA is pursuing a dual-track program. On the one hand, it is looking for devices that, while limited in effectiveness, have the advantage of being avail-

[5] The final OTA report will discuss this issue in detail.

[6] For a discussion of why it takes so long to field the results of government-funded R&D, see U.S. Congress, Office of Technology Assessment, *Holding the Edge: Maintaining the Defense Technology Base,* OTA-ISC-420 (Washington, DC: U.S. Government Printing Office, April 1989), ch. 8.

able soon. On the other hand, it sponsors technology that is not yet mature, but has the promise of producing superior equipment in the long run. The FAA's funding has increased substantially in the last 2 years, as Congress has urged increased research efforts in hopes of providing a near-term solution.

The FAA's work in sponsoring research appears to be improving, in part due to increased funding, which makes it possible to take more research risks. But there is a need to decide with some firmness on a date, preferably within 2 years, by which time competing technologies for near-term application should provide detectors to be tested in realistic settings. This would allow the winnowing out of unpromising lines of research. If testing is successful, a rule requiring widespread acquisition of the detectors could be promulgated. This action would presumably stimulate the market to produce more competing instrumentation of the same type. If testing in a given area is unsuccessful, this may indicate that R&D should no longer be actively supported along that particular direction.

If such a restriction is not imposed on research that is on the near-term track, there is a danger that technologies may continue to develop, but without ever producing workable prototypes. It is a cliche, but true, that the better becomes the enemy of the good.

One difficult task is to formulate a reasonable set of performance standards to judge the products of research. The standards will have to be acceptable to Congress, as guardian of the public interest.[7] If this had been done in the TNA case, much controversy and many political difficulties could have been avoided. There are, however, problems in setting standards, particularly for vapor detectors, because the performance of the machines is so affectedly the scenario in which they are used and, thus, a terrorist scenario must be specified in order to set the standards. Efforts have been made in developing such scenarios, e.g., by the American Society for Testing and Materials, but little in the way of progress has yet been achieved. Nevertheless, a logical basis for standards must be developed and set so that credible testing and evaluation may begin.

Analysis is needed to determine how much effort should be devoted to developing near-term solutions, how much to longer term technologies, and how much to accelerating work on the more promising longer term technologies so that they may be developed more quickly.

FAA RULEMAKING FOR EXPLOSIVES DETECTION SYSTEMS

The FAA accepted a TNA prototype in fulfillment of an R&D contract following a series of tests run in 1987 and 1988 at Los Angeles and San Francisco Airports. These tests have been criticized by a number of groups.[8] They were not double-blind and they used explosive simulants equivalent to the amount then thought required to cause a large commercial aircraft to crash. Unfortunately, after Lockerbie, the world discovered that a much smaller quantity could destroy an aircraft. Further, the explosives were attached to the outside of test items of luggage, not a likely geometric configuration to be found in practice.[9]

As part of Public Law 101-45, which became effective on June 30, 1989, Congress ordered FAA to develop a rule that required:

> . . . 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 FAA then issued a proposed rule, published in the Federal Register as a Notice of Proposed Rulemaking, to amend part 108 of the Federal

[7] The specific details probably should be kept secret from the public to avoid tipping Off terrorists as to the limitations of the accepted systems.

[8] For example, seethe testimony of Ref. Lee Grodzins before the Presidential Commission on Airline Security and Terrorism, Washington DC, Feb. 9, 1990.

[9] This is another serious defect, since the TNA system is supposed to ''learn,'' through an artificial intelligence technology known as ''neural networks," to detect a bomb in a suitcase through experience in evaluating data (stimulated gamma ray counts from the suitcase, together with the rough location of the gamma rays' origins) and comparing it with the knowledge of whether the suitcase actually had a simulated explosive or not. If the samples on which the device learned were not realistic, there would be no guarantee that, when inspecting realistically packed bags containing explosives, the machine would have the same rate of detection or false alarms.

Aviation Regulations to require an explosives detection system (EDS) for screening checked baggage (but not carry-on baggage) on international (but not domestic) flights.[10] Ironically, TNA might work better for carry-on than for checked baggage because the weight of carry-on luggage is generally less than the weight of checked luggage. Thus, for carry-on luggage, the nitrogen signal from the explosive would be easier to see above the background from other nitrogen in the bag than would be the case for checked luggage. About half of recent successful airline bombings have resulted from explosives placed in the passenger compartment, and half from explosives in the cargo hold.

The EDS was supposed to alarm automatically. This feature was designed to eliminate reliance on security personnel for a rapid determination of what was suspicious and what was not. Many security personnel are not highly paid, trained, or motivated, and reliance on their alertness under these constraints was not considered to be reasonable.

The Final Rule was published in early September 1989.[11] The FAA felt that it was feasible to promulgate and enforce the rule since the tests at the two airports showed that at least one technology was available. In the discussion accompanying the Final Rule, the FAA referred to TNA as "the only existing, proven system. ' The goal, as stated in the Final Rule, was to require 860 such systems by 1999. An alternative possibility was to install 200 within 3 years and 300 by 1999.

In further tests carried out at JFK Airport in New York since September 1989, the TNA system has performed significantly worse than in the earlier tests. In addition to frequent calibration tests done with simulated explosives on the outside of luggage, the JFK tests are also occasionally performed with explosives placed within bags taken from a set belonging to the FAA for test purposes. This latter test is claimed to have been carried out in a double-blind manner.

Whereas detection probabilities of 95 percent with false alarm rates of 5 percent were cited from the earlier tests, more recent results quote significantly higher false alarm rates. Further, at least one common explosive used by terrorists was not simulated and **used for testing the device. The** false alarm level was reduced by adding a two-beam x-ray device to the equipment. However, the rate was still high enough to clog airport operations, if the device were to be used to screen every piece of baggage.[12] Automated decisionmaking was not used for the x-ray part of the equipment. In any case, for a Lockerbie-sized bomb, which was smaller than equivalent explosive quantities used in the initial tests, the detection rate is likely to be much worse, or the false alarm rate higher (or both) than the figures cited above.

Based on the testing results up to the present, the TNA device by itself does not currently appear to be an adequate **system for screening baggage at airports for small but deadly quantities of explosives. On the** positive side, the experience gained by installing an explosives detector in an operational environment has been extremely valuable and has provided the FAA with important lessons that will help in developing performance criteria as well as evaluation standards and procedures for future EDS devices.

Attention should be given to developing means (TNA-based or other) of screening carry-on baggage. TNA may work better in this mode than for checked baggage.

---

[10] Federal Register, 54, p. 28985, July 101989.

[11] Federal Register, 54, p. 36938, Sept. 5, 1989.

[12] It is difficult to say without a detailed analysis what an acceptablefalse-alarm rate would be. Some estimates, however, may be made. A false-alarm rate of 5 percent is required by the FM rule. However, even this rate maybe marginal at busy airports, in that long queues maybe generated. A recent study for the Air Transport Association gives support to this view (Practicability of Screening International Checked Baggage for U.S. Airlines, Geoffrey D. Gosling and MarkM. Hansen, Institute of Transportation Studies University of California at Berkeley, UCB-ITS-RR-90-14, July 1990). As mentioned in an earlier footnote, one foreign country has found it possible to operate if about 3 percent of checked baggage is carefully inspected, so a false-alarm rate of this level would be tolerable in at least some circumstances.

Appendix A
Nuclear-based Explosives Detection Systems

Thermal Neutron Analysis (TNA)

Sponsor: Federal Aviation Administration (FAA) Technical Center through contractual relationship with Science Applications International Corp. **(SAIC).**

Status: Testing of one preproduction unit is under way at JFK Airport, New York, one unit was recently checked out in Miami, one is at Dunes, one at Gatwick and two more are to be delivered to FAA shortly for installation at selected airports in the United States and abroad.

Funding: $12 to $15 million R&D funding over 4 years from FAA Technical Center, plus about $5 million private funding, plus $15 million for the six preproduction units FAA bought for airport demonstration.

Basic Operating Principle and Goals of Concept

When a neutron strikes a nucleus, there is a certain probability that it will be absorbed. This process is often accompanied by the emission of a high energy gamma ray whose energy is characteristic of the nucleus. The amount and type of some specific elements present in a sample inspected by neutron radiation can be inferred from a measurement of the intensity and energy of these gamma rays. The TNA concept depends on this principle for the identification of nitrogen in explosives.

An item of luggage is moved through a "bath" of thermal (i.e., slow) neutrons generated by a radioactive source or an electronic neutron generator (particle accelerator). In the current design, the isotope californium-252 is used. The capture of a neutron in nitrogen results in a high-energy gamma ray produced through the reaction

$$^{4}N + \text{thermal neutron} = \ ^{5}N + 10.8 \text{ MeV gamma.}$$

The signals from an array of gamma-ray detectors are analyzed to give a rough spatial distribution of nitrogen. Figure A-1 demonstrates the principle of operation of TNA.

The currently tested version of TNA was designed, following FAA performance specifications, to detect a minimum mass of nitrogen, equivalent to a certain quantity of plastic explosives. It has limited spatial resolution and detects primarily nitrogen, not oxygen or carbon; although hydrogen, chlorine, and some other elements could, in principle, be detected to enhance performance. Because only nitrogen is currently specified by the device and because of the system's difficulty in dealing with nitrogen background from innocent materials, the false-alarm rate is higher than desired. This has become an important issue for the current TNA hardware. Further, the sensitivity (probability of detection for a given quantity of explosives) is limited. Sensitivity can, indeed, be increased by lowering thresholds, but a concomitant rise in the false alarm rate results. This situation can be improved, according to the system's designer, by using TNA or other techniques to measure other elements present and by other system modifications.

Technical Description

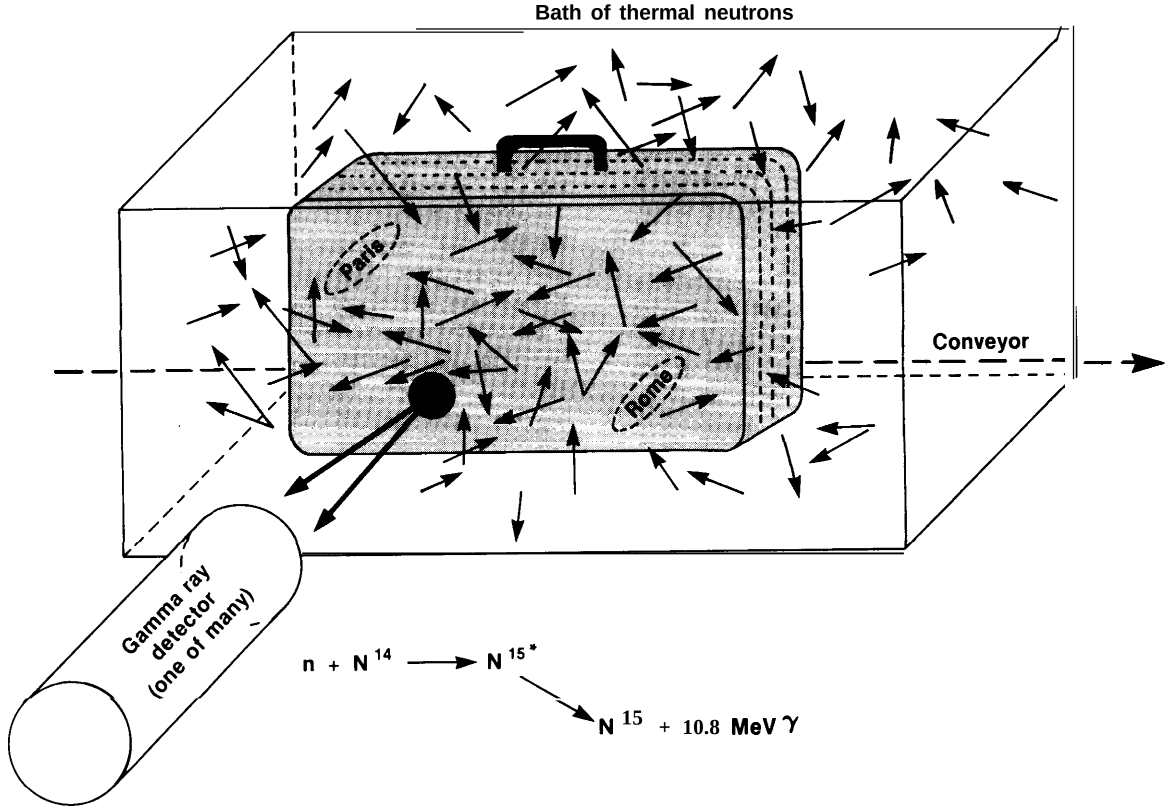
The current TNA equipment is represented by engineered preproduction units that are being tested at airport sites. They are being modified and upgraded in accordance with experience gained in a real operating environment. For instance, an x-ray system has been combined within the TNA set-up in an attempt to reduce the false alarm rate. The combined TNA/x-ray system is generally referred to as the "XENIS' system.

The californium source is of moderate strength (approximately 80 millicuries or 3 x 10^9 alpha particles/see and 3.5 x 10^8 neutrons/sec[1]). It is contained in a small, double-walled capsule of a common industrial design. The capsule was exposed to a blast from a substantial explosive charge and maintained its integrity. Radiation from the shielded system, near its surface, has been examined and found to be comparable to the natural background level of radiation exposure. The environmental threat of the system has been assessed by the Nuclear Regulatory Commission (NRC) and found to be within Environmental Protection Agency and NRC exposure guidelines.

The source exposes baggage on a conveyor belt to a "bath' of neutrons inside a shielded cavity. The baggage is surrounded by an array of gamma-ray detectors, which send their data to a computer. The software, in turn, transforms the data into" a spatial distribution, giving a rough image of the nitrogen content of the object. The system also records various other data used as input to algorithms that distinguish objects that contain explosives from "clean" ones. The details of the analysis algorithms have not been examined by OTA. Generally speaking, the system utilizes artificial intelligence techniques based on neural networks and permit the system to learn from experience. Many pieces of baggage, including both items containing explosives and clean ones, are observed by the

[1]A curie is 3.7x 10^{10} disintegrations/sec

Figure A-l—Sketch of Apparatus for Thermal Neutron Analysis of Nitrogen



SOURCE: Lee Grodzins, 1990.

system in order to learn the distinguishing characteristics of the "bad" objects.[2] There is a continual upgrading process in refining the decisionmaking algorithms. The add-on x-ray system is used to reduce the number of false alarms by determining whether the nitrogen image (provided by TNA) overlaps with the two-dimensional image of density (given by the two-view x-ray system used). The details of the correlation of these data have not yet been examined by OTA.

Status

The current version of the TNA device was developed by SAIC under FAA Technical Center sponsorship during the last 5 years. SAIC was selected by a competitive procurement process in 1985. The current device was designed to satisfy performance specifications set down by FAA at that time. These demanded, among other things, a baggage handling rate of 10 per minute (6 seconds per bag) and automated detection. The devices were tested against these criteria at SAIC's laboratories at Santa Clara, CA, as well as at San Francisco (SFO) and Los Angeles (LAX) Airports in 1987 and 1988, where the system was accepted by the FAA as meeting these specifications. These tests were not done independently, but were designed and conducted jointly by the FAA and SAIC, in the presence and with the concurrence of FAA consultants. This test was performed somewhat in the manner of some Department of Defense weapons acceptance tests, and there is currently considerable controversy over their significance.

Since that time, the FAA has ordered 6 preproduction units from SAIC for actual airport testing at a cost of about $15 million. This price includes SAIC's participation in operations, maintenance for 1 year, and installation, including the x-ray adjunct. The last of these units are scheduled to be delivered to the FAA when their destinations are determined. Currently, three of these units are operative, one at Trans World Airlines (TWA) at JFK Airport in New York, one at Gatwick Airport, near London, and one at United Airlines at Dunes Airport in the Washington, DC area. A fourth is being refurbished after a year's operation at Miami International Airport at Pan American Airways. The Kennedy system routinely operates about 5 hours per day, during which time most of the foreign flights leave New York. It examines about

[2] The original selection algorithm was based on SAIC's lost luggage stock. Later it was amplified by the experience gained at Los Angeles and San Francisco airports. The system is currently using the experience it is gaining at various sites to refine its decisionmaking capability.

350 bags per day, primarily the interline transfer bags from other flights. This selection was based on logistic considerations (i.e., where the system could be physically placed in the TWA baggage handling area), and is the limiting factor on the testing of the system's throughput capacity. The Miami system was located at a baggage transfer point and the Gatwick and Dunes units are located in the main concourse in front of the check-in counters.

The system is tested daily against baggage containing simulated explosives. Performance data are gathered from these tests as well as from the false alarms of real passenger luggage. The current false-alarm rate is running higher than that achieved in the "acceptance" tests for the "LAX distribution.' The XENIS system uses a two-view x-ray seamer system, built by EG&G Astrophysics Division, in tandem with the TNA device. With this combination, the false-alarm rate is lowered significantly. Any bags that do not pass the TNA/XENIS system and are still deemed suspicious, following a close examination of the data by an operator, are turned over to TWA for further action. It has been claimed by SAIC that by rerunning a suspect bag, the false-alarm rate can be lowered to a very few percent. However, SAIC also notes that this decreases the probability of detection.

The algorithm by which the system either accepts or rejects a given bag is still under development and is being modified to include the x-ray information. In the current operating version, the x-ray/TNA information match is being performed outside of and independent of the TNA analysis.

Potential and Shortcomings

The SAIC TNA is the first automated baggage inspection system and the only one that, in the view of the FAA, meets present FAA guidelines. However, the degree to which it meets these guidelines is very controversial. The impartial testing of this baggage handling system is a complex issue: many variables need to be considered. Baggage differs among airports, flights, and seasons. These differences have profound effects on system performance. Explosives also differ greatly. Various types present differing degrees of difficulty. Also, human factors are involved in how the explosives are handled for any test. Currently, there is no generally acceptable test protocol that would allow the FAA to certify that a system is "working properly", although FAA contracted with the Department of Energy's Sandia National Laboratory to propose one. The National Research Council is also looking at this issue for the FAA.

The current TNA system also has several severe shortcomings, including its high cost, which is currently estimated to be $0.75 to $1.0 million per system (depending on various assumptions including the savings due to large-scale production). SAIC claims to be willing and able to build 30 units per year, but so far has no committed orders and currently plans to build only a few beyond the past FAA purchase. The current system is massive, weighing close to 14 tons and taking up a large amount of real estate (the footprint for the TNA alone is about 12 m^2, and an additional equivalent area would be needed to add an x-ray system and baggage diverter) in an area where space is scarce and valuable. Considerable site preparation was necessary for the JFK installation. Further, the use of a radioactive source and the resulting shielding requirements present an acceptance problem. If an electronic neutron generator were used, the shielding requirement would not be reduced. To date, foreign acceptance of TNA systems has been difficult to achieve, but there are active negotiations between the FAA and some foreign airports for test systems, and, as noted, a TNA unit has been installed at Gatwick, near London.[3]

The limited sensitivity and the strong dependence of the false-alarm rate on the lower limit set for detection is one of the major issues that will determine the utility of the current version of TNA. The sensitivity, in terms of the detectable amount of explosive, was set by the FAA prior to the Pan Am 103 incident at Lockerbie, which is generally thought to have resulted from a substantially lesser amount than the original FAA specification.[4] The publicly available data taken to date on the issue of threshold sensitivity v. false-alarm rate are sparse.[5]

[3] The radiation exposure issue appears to be one of perceptions; the facts do not appear to indicate a serious problem. The operators of the TNA will be shielded to levels that are acceptable for workplace exposure, as defined by Food and Drug Administration standards (at 1 foot from the system, the radiation level is less than the permissible levels allowed for home TV sets). Residual dose rates from the baggage are very low—0.03 microSv/hr at the surface immediately after exposure. The radioactivity declines rapidly afterwards. For comparison, a resident of Leadville, CO experiences an exposure of 2.8 milliSv/yr, transcontinental airline crews experience 2.80 milliSv/yr in addition to exposures received from normal background (which amount to about 1.5-3.0 milliSv/yr, depending on location), the average human receives 0.2 milliSv/yr from potassium in food. Eating one banana per day gives a dose of 0.8 microSv/yr. From these&@ it would appear that the danger from radioactivity from TNA is not a real issue.

[4] However, there were several cases many years prior to Lockerbie in which lesser amounts of explosive were introduced aboard the aircraft cabin and produced significant damage and fatalities.

[5] At an NAS Symposium on Airline Security and Explosives Detection, Feb. 26-27, 1990, Dr. Gozani of SAIC reported that when the sensitivity was raised to maintain a 95 percent detection probability for this reduced amount, the false alarm rate rose to a high level. Since the initial writing of this report, a significant amount of new testing of the TNA/XENIS systems both at Santa Clara and at JFK has occurred. Some of these tests were run by SAIC with FAA supervision and overview, some by the FAA, and the last set by a group of independent consultants hired by the FAA, headed by Dr. Joseph Navarro of Wackenhut Securities Co., supported by representatives from Sandia National Laboratory, the National Institute for Standards and Testing, and the University of Georgia.

Although the SAIC TNA system is the only FM-‘‘accepted’ explosives detector currently at the prototype stage, there is considerable commercial interest in the development of more advanced versions of TNA. The FAA rule, requiring installation of an explosives detection system (EDS) at 40 U.S. airports over a 3-year period following the issuance of a final ruling, creates considerable incentive to industry to compete with SAIC. At approximately $1.0 million per unit, this would represent a $200 to $300 million market over the next several years. Several domestic and foreign firms (e.g., Gamma-metrics of San Diego), experienced in building similar inspection equipment, are seriously eyeing this market and are engaged in active development work to define their concepts, and SAIC is working to improve the performance of their system. It is possible that within a year or two, several such systems may be available for certification, possibly with some advanced features or options.

Another aspect to consider is the potential for TNA as a detector for explosives in carry-on baggage. Checked bags contain nitrogen in widely ranging amounts. The task of finding a small bomb against this varying background is very challenging. It is necessary to use information on the spatial distribution of nitrogen density to reduce the false-alarm rate even to its current high level. Since carry-on bags tend to have less mass than checked bags, the background would usually be less and the detection task easier. It would be useful to pursue this option, especially because now, only x rays are used to screen carry-on baggage, and it is extremely difficult, even for highly trained experts, to find a bomb using only standard x-ray images.[6] Some preliminary studies have been carried out on this problem by SAIC.

Fast Neutron Analysis (FNA)

Sponsor; FAA Technical Center is supporting some work at SAIC; there is some commercial development.

Status: Pre-prototype development.

Funding: $600,000 from FAA to SAIC for basic feasibility demonstration and preliminary conceptual design.

Basic Operating Principles of the Concept

As an improvement on TNA, more energetic neutrons can be utilized to give more information. When the slow neutron source of the TNA is replaced by a more energetic one, the interaction of the energetic neutrons with the nuclei of the elements in the object to be examined will produce gamma rays at different energies, characteristic of the elements, which can be detected and distinguished. These are often more copiously produced and thus easier to see above background than the gamma rays produced by thermal neutron irradiation. For instance, 14-MeV neutrons interacting with oxygen, carbon, and nitrogen will produce 6.1, 4.4, and 5.1 MeV gamma rays respectively. Measurement of each of these separately (see figure A-2) may yield a rough spatial distribution of the three elements in a manner similar to the TNA system.

Technical Description

An FNA system is physically similar to the TNA system, but there are significant differences in the source, the shielding requirements, and the gamma-ray detection arrays. A fast neutron source requires an accelerator, not a radioactive source, and is thus significantly more expensive from the beginning (at least by $250,000 and probably considerably more). An FNA system will almost certainly require more shielding than the TNA, representing another potential increase in cost, size, and weight. Several different concepts of fast-neutron sources are under development both in the United States and abroad (notably France). Many more elements, most importantly oxygen, can be measured by this technique.

Potential and Shortcomings

The obvious potential of the FNA is that it makes an essentially unambiguous determination of the presence of common explosives. It was shown in figure 4-4 that common explosives display a nearly unique range of nitrogen density to oxygen density. By being able to measure both these quantities as well as carbon and hydrogen density, FNA should greatly improve accurate identification of a hidden threat.

On the other hand, an obvious shortcoming of the FNA system is the use of fast neutrons. These neutrons create a significant background in the gamma-ray detectors, making it difficult to extract the information. The feasibility of commercial use of such a source, its shielding, and consequently, its operational restrictions in an airport environment have yet to be established, though a significant body of data from laboratories and from bore-hole oil-well logging does exist.

Pulsed Fast Neutron Analysis (PFNA)

Sponsor: FAA Technical Center.

Status: Basic R&D and feasibility experiments in progress under FAA sponsorship.

Funding: *$220,000* from FAA to SAIC

---

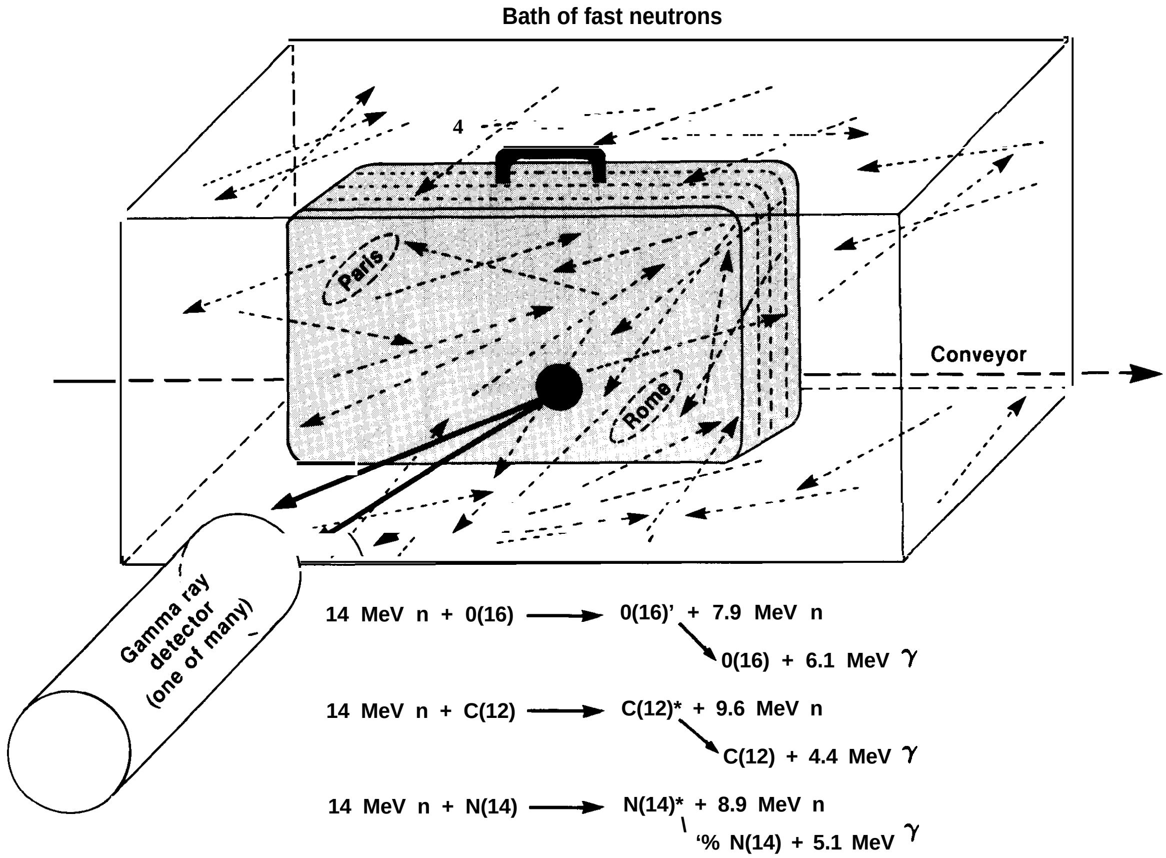
[6] The detailed results vary with many parameters, but several general characteristics are repeatedly seen. The following statements should be kept in mind when considering TNA/XENIS test results:

. Detection Probability, P_D, is generally given as a weighted average for a specified selection (usually 5) of different explosives.

. When thresholds are reduced, false alarm rates rise rapidly.

Another adjunct to x rays for screening carry-on baggage could be advanced vapor detection systems, now just coming on the market.

Figure A-2-Sketch of Apparatus for Fast Neutron Analysis of Nitrogen, Carbon, and Oxygen



SOURCE: Lee Grodzins, 1990.

Basic Principles of Operation of the Concept

The PFNA concept is similar to the FNA system, except that a pulsed beam of neutrons is utilized. A focused, collimated beam is passed through the object, resulting in the emission of gamma rays of specific energies, characteristic of elemental constituents of the sample. This method uses penetrating neutrons at lower energies than in FNA. At these energies, the probability for gamma-ray production by nuclear reactions with oxygen, carbon, chlorine and nitrogen is about the same as for 14 MeV neutrons; however, the gamma-ray spectrum is cleaner and shows a much better signal-to-noise ratio. The gamma-rays are detected, as before, by scintillators that provide gamma-ray energy information by which the element can be identified. The neutron beam profile provides the two-dimensional position information required to determine the spatial distribution. The third dimension, derived by timing and image reconstruction, constitutes a significant improvement over the basic FNA technique. A schematic view is shown in figure A-3.

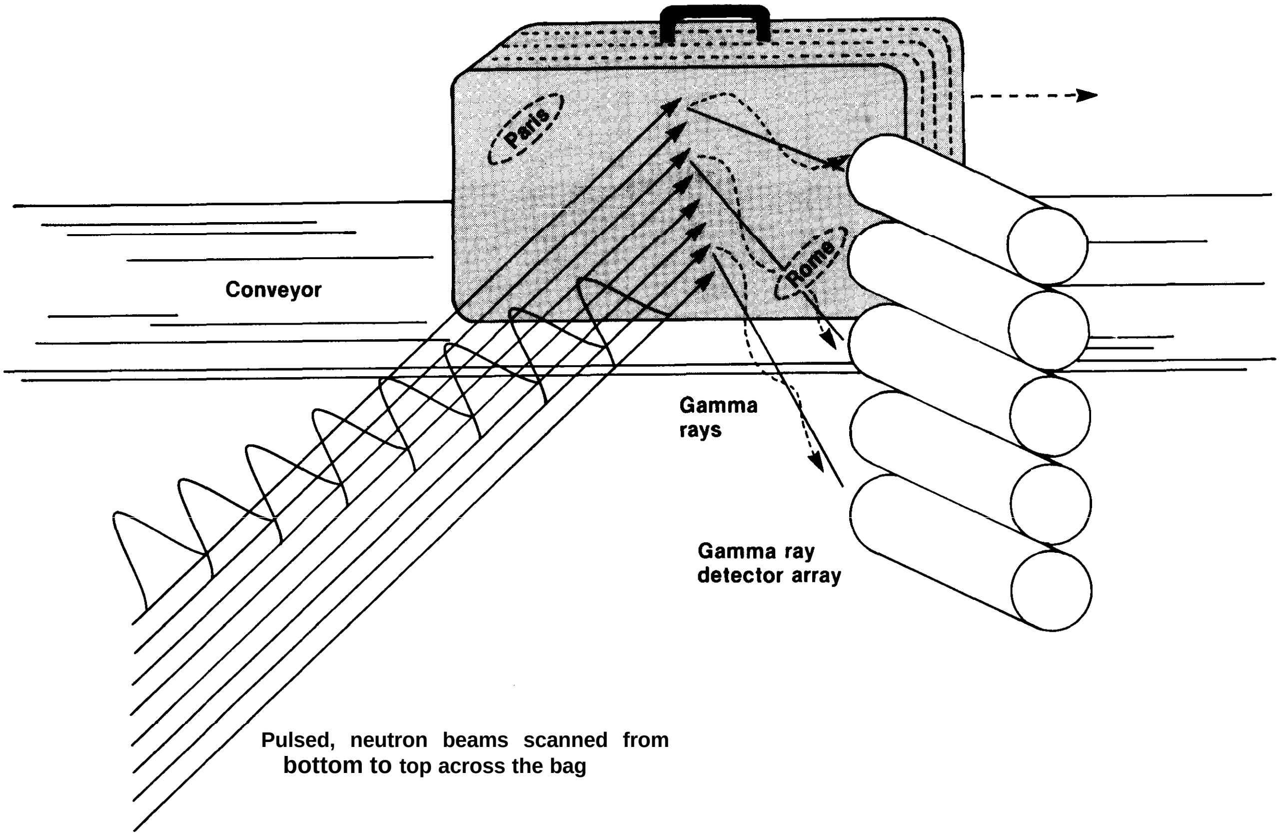
Technical Description

Neutrons are generated by a pulsed accelerator in precisely timed bursts. The arrival of the gamma-rays is also accurately timed. The position of "interaction along the neutron beam is determined using the time interval between these pulses and the neutron speed, giving a third dimension to the element density distribution.

The neutrons are generated by the deuterium-deuterium (d-d) reaction and produced mainly in the direction of the deuteron beam. The accelerator is larger and more expensive than the deuterium-tritium (d-t) neutron generators used in FNA, due to their higher voltage.

preliminary studies have demonstrated the feasibility of determiningg the position of the elemental constituents of different samples. Better accuracy is expected with the use of shorter duration deuteron beams and gamma-ray detectors with better temporal resolution. Pulsed d-t generators could also be used instead of continuously operating ones with the main advantage of lower acceler-

Figure A-3-Sketch of Apparatus for Pulsed Neutron Beam Analysis



SOURCE: Lee Grodzins, 1990.

ator cost, size, and weight. However, they present a poorer signal-to-noise ratio and require heavier shielding.[7]

Potential and Shortcomings

The attraction of the PFNA system is its unambiguous determination of the elemental composition characteristic of explosives and the spatial information on the location of these elemental concentrations. These features make the PFNA a potentially powerful technique for explosives detection.

To date, only the basic feasibility of PFNA has been established. The R&D required for the construction of a practical, collimated, pulsed energetic neutron beam, however, is a technological problem, and the requirement for making it safe and operationally acceptable, as well as cost-effective, complicates the matter. The PFNA system represents a considerable research and development problem, likely requiring 3 to 5 years before its commercial utilization can be assessed. A thorough evaluation of the operational issues of such a system should precede the large expenditures-for cost, space, performance and accelerator safety-that would be required to develop such a system.

Nuclear Resonance Absorption (NRA) of Gamma-Rays

Sponsor; FAA Technical Center is supporting research at LANL and the Israel Atomic Energy Commission Nuclear Research Center at Soreq.

Status: Feasibility experiments completed in Fall 1989, more research funding is likely.

Funding: About $l million in fiscal years 1988 and 1989; requests for a program of $1 to $3 million per year for the next 2 to 3 years are under discussion.

Basic Operating Principles and Goals of Concept

Physicists at the Soreq Nuclear Research Center of the Israel Atomic Energy Commission proposed a scheme to the FAA in 1986 in which the presence of nitrogen would

[7]This description owes much to the comments of T. Gozani of SAIC.

be detected by measuring the absorption of gamma rays traversing a piece of baggage. The probability of absorption of the gamma rays of a particular energy by nitrogen nuclei is very high. Scintillators would detect the transmitted gamma rays. A dip in the detected gamma rays would indicate presence of nitrogen in the baggage.

The technique is derived from the existence of a narrow state of excitation energy in ^{14}N, resulting in a sharp resonance of the cross section for the reaction $^{14}N(\gamma,p)^{13}C$ producing a proton and a ^{13}C nucleus. The gamma-ray transition rate from the ground state of ^{14}N to the excited state is extraordinarily large. This means that gamma rays of exactly the resonant energy are very strongly absorbed by ordinary nitrogen nuclei, thus providing a unique and clear signature of the presence of nitrogen, as opposed to other elements.

The inverse reaction (protons on a target of ^{13}C nuclei) can be used to generate the probing beam of gamma rays, resulting in gamma rays of just the right energy for the subsequent resonance absorption. The effective size of the source of these gamma rays can be made very small, allowing an imaging capability. This technique has been demonstrated to be capable of detecting nitrogen at levels similar to FAA's current requirements. Since the signature is unique and the gamma rays very penetrating, the technique is impervious to attempts to avoid detection by shielding the explosives.

Technical Description

The geometry of the NRA technique is very similar to the familiar x-ray systems used at airports. However, instead of a fan shaped beam of x rays, one uses a fan shaped beam of gamma rays at precisely the right energy to pass through the luggage (see figures A-4 and A-5).

A small electrostatic accelerator produces a proton beam. When a beam of low energy protons, produced by a small electrostatic accelerator, hits a ^{13}C target, the residual ^{14}N is produced in the desired excited state. From this state, high-energy gamma rays are produced the great majority of the time (the balance being low-energy gamma rays). At one particular angle with respect to the proton beam, the energy of the gamma rays is exactly what is required by the resonant absorption in nitrogen. The beam spread depends primarily on the spread of energy in the proton beam, the quality of its focusing, and the thickness of the carbon target. The beam spread and various other parameters of the apparatus have been measured in the completed feasibility program to determine the practical performance limits of the concept.

In addition to the proton-beam/accelerator, the apparatus consists of a thin, cooled target and a detector array aligned precisely to intercept the cone of gamma rays which are emitted at the optimum angle. There are two choices of detectors under consideration, resonant detectors favored by Soreq investigators and nonresonant detectors proposed by a group from LANL that has cooperated with the Soreq group in the program. Each of the schemes has its advantages and disadvantages and a clear choice is not obvious at this time. The nonresonant detector is much more efficient and is commercially available, but must sort out resonant absorption (specific to nitrogen) from a nonspecific background. The resonant detector needs developmental work, has lower inherent efficiency, but produces a more unambiguous signal.

Measurements have been made, both with a nonresonant detector (a commercial BGO scintillator) and with a resonant detector array. In both cases, luggage with simulated explosives was passed through the beam of gamma rays in front of the detectors. Images were formed by computer reconstruction of the data from the detectors, creating an array of pixels. The total nitrogen was obtained by summing over all the pixels. When the total nitrogen content was above some critical quantity, an image was constructed to give the distribution and location of the nitrogen. Explosive samples were detected with very small amounts of nitrogen, either in blocks or sheets and hidden within a radio. Impressive images of simulated explosives have been obtained, using computer image-enhancement techniques. The experiments that were performed have been used to design potential prototype systems that would be able to handle the FAA requirements for an airport luggage inspection system.

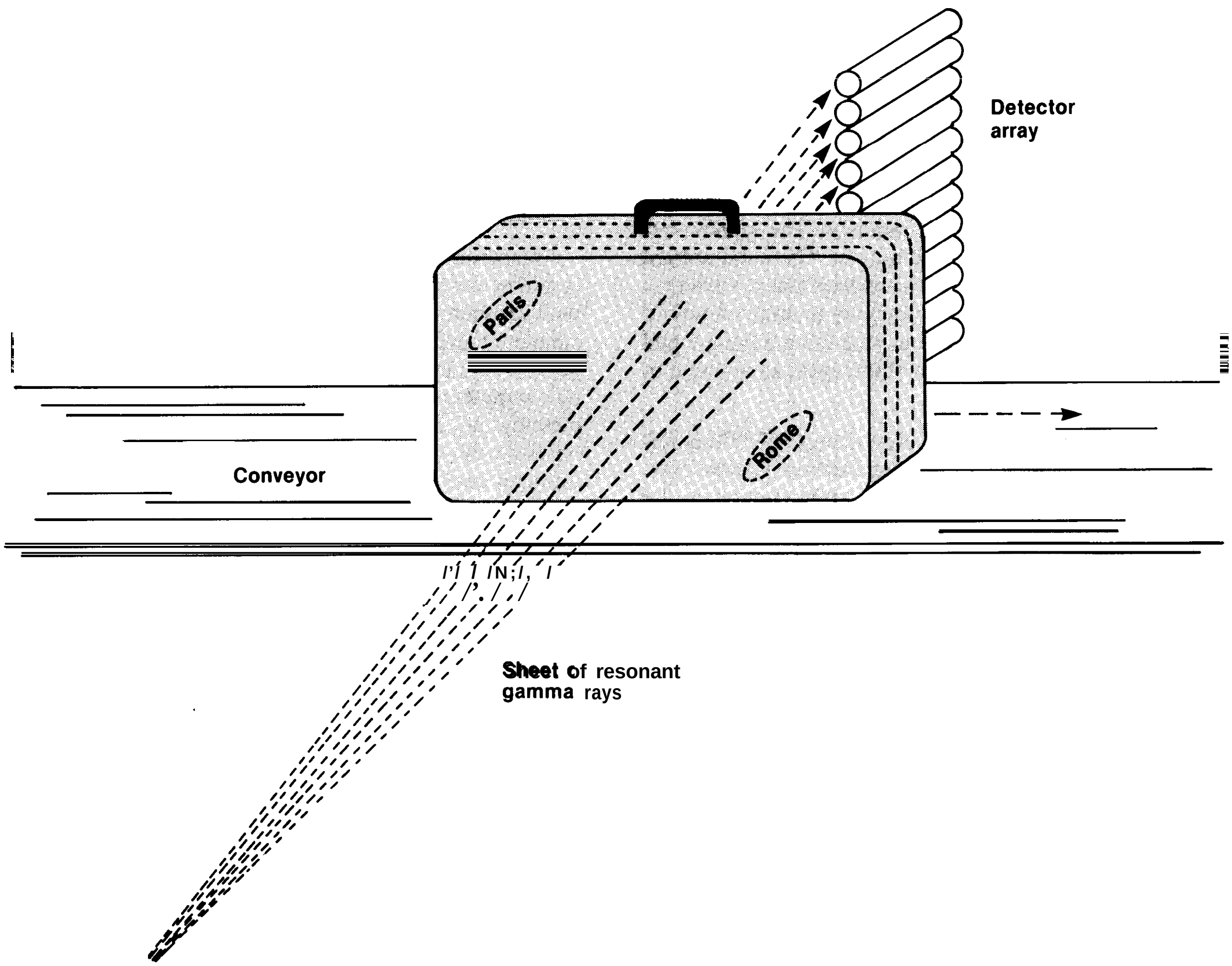
Potential and Shortcomings

The NRA system may have considerable potential for the FAA luggage explosive detection system (EDS) mission. It appears to have the needed sensitivity and spatial resolution and it measures nitrogen unambiguously. However, like the current version of TNA, it does not measure anything but nitrogen.

The major choice that needs to be made at this time is the level of investment in this technology and the program emphasis for the immediate future. The question is, should the program be aimed at demonstrating this technology in the near term with a pre-prototype device, based on currently available hardware, that can be operated in an airport environment, or should the program be aimed at assessing the ultimate potential of this system (higher sensitivity with low false-alarm rate) in the long term, or should money be made available for both?

Even if a major program based on this technology were to be initiated, it would take about 2 years to demonstrate the technology in the field and another 2 or 3 years before an optimized system could be made available to the airlines. At best, this could be cut to 3 years on a fast-track high-risk (probably greater than about $10 million) program, directed immediately at an advanced performance system.

Figure A-4-Resonant Absorption of Gamma Rays



SOURCE: Lee Grodzins, 1990.

There are no good estimates of the cost, size, weight, and operating parameters that could be expected from such a system and a paper study aimed at determining such parameters under various technology assumptions could be valuable. In making a cost comparison with the TNA system, the NRA's accelerator will most probably be significantly more expensive than the current isotopic source for TNA. Some of this increased cost maybe made up by less expensive shielding (since gamma rays are easier to shield than neutrons, and the 1.747 MeV protons have too low an energy to induce much radioactivity in the apparatus) and a cheaper detector system. The resonant absorption technique is one of the more promising advanced technologies and such a study could quantify its potential.

Associated Particle Production

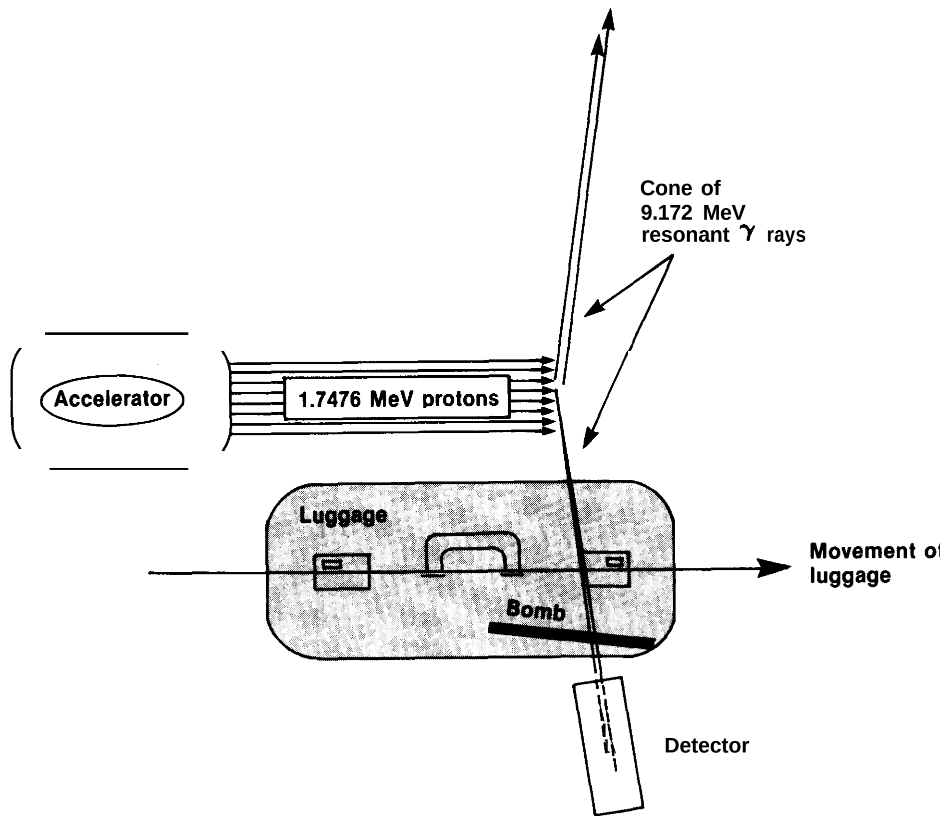
Sponsor: FAA Technical Center—DOE at Los Alamos National Laboratory, previously sponsored by TSWG.

Status: Early Research.

Basic Operating Principles

The technique uses high energy (14 MeV) neutrons and 3 MeV alpha particles from a deuterium-tritium reaction. The direction and timing of the alpha particles are

Figure A-5-Resonant Absorption of Gamma Rays



SOURCE: Lee Grodzins, 1990.

measured to determine uniquely the direction and timing of the neutrons. The timing and energy of the gamma rays that result from the interaction of these neutrons with the nuclei of the examined object are also measured. By combining the gamma-ray data with the alpha-particle and time-of-flight information, a three-dimensional mapping of the carbon, nitrogen, and oxygen in the baggage may be obtained. The spatial resolution of this system should be adequate to see small explosives.

This technique is another one that has the potential to provide an unambiguous and spatial determination and, consequently, should be highly effective for detection. Preliminary experiments have been performed at LANL with promising results, but fielding this technology would not be likely for many years.

Nitrogen-13 Production-Positron Emission Tomography

Sponsor: DARPA, in cooperation with Sandia National Laboratories, supporting Titan Corp. (Spectron Division).

Status: Funded demonstration program.

Funding; $2.83 million over three years, of which $1.78 million went to Titan from DARPA, and $1.05 million went to Titan from Sandia.

Basic Operating Principles:

In this technique, a gamma-ray beam activates the ^{14}N isotope[8] in explosives to an excited state of a radioactive isotope of nitrogen (^{13}N). A neutron is also emitted, which is not important for this application. The reaction is:

$$\text{gamma-ray} + {}^{14}N = {}^{13}N^{*} + n.$$

Following activation, the nitrogen-13 isotope decays with a ten-minute half-life, emitting positrons (the positively charged antiparticle of an electron). Each positron immediately annihilates with an electron in the region, producing two back-to-back 511-keV photons that are detected by scintillation counters.

The gamma-ray beam is produced by a specifically designed radio-frequency linear accelerator (RF-LINAC).

[8] In nature, over 99 percent of nitrogen exists as the isotope ^{14}N with the balance being ^{15}N.

The accelerator first produces an electron beam of about 14 MeV energy. The electrons then strike a tantalum or tungsten target and produce gamma radiation with a maximum energy equal to that of the electron beam. The gamma rays interact with explosives and activate the nitrogen via the above photonuclear reaction.

One advantage of this approach is that, by tracing back the paths of the two 511-keV photons, one can achieve excellent spatial resolution, perhaps on the order of a centimeter or so in each dimension.[9] The ability to image will be vital in order to eliminate background coming from those few isotopes that might confuse the picture.[10] A final assessment on how well this system can get rid of background awaits the testing of a prototype.

One of the features of this system is that, because of the 10-minute half-life of the radioactive nitrogen isotope, the irradiation and detection stations can be separated, reducing background problems and simplifying detection. Further, it is easy to have multiple detector stations for each radiation source (the accelerator). It is proposed to use this system in tandem with standard x-ray seaming or tomography equipment to achieve high resolution.

Status

This technique, designated by the vendor as Explosive Detection Using Energetic Photons (EXDEP), has been experimentally checked in the laboratory for detection of buried mines. A demonstration system is currently under construction at Titan for testing in realistic situations. An aggressive program aimed at the FAA mission would probably require about 3 to 4 years, and $5 to $10 million. As with other energetic particle beam concepts, the accelerator, its cost, size, and shielding requirements are major issues.

Pulsed Neutron Backscatter (PNB)

Sponsor; Commercial development to date by PENETRON, Inc.

Status: Some laboratory measurements made to verify concept

Funding: Proposal submitted to FAA under Broad Agency Announcement.

Basic Operating Principles

The PNB concept is based on the fact that fast neutrons will interact frequently with light nuclei by elastic collisions (roughly equivalent to billiard balls bouncing off each other). Since the collisions are elastic, there is no change in the structure of the nucleus; rather, the neutrons scatter in particular directions with unique reduced energy determined by the mass of the nucleus hit. Thus, by measuring the energy of the scattered neutrons, the nucleus that had been struck can be identified.

Two physical phenomena are used to detect and analyze remotely concealed substances, such as explosives and narcotics. One is Neutron Elastic Back Scatter (NEBS) and the other is Neutron Resonant Elastic Scatter NRES).

In NEBS, carbon, oxygen, and nitrogen all produce different back-scatter velocities. The intensity of the back-scattered signals contains information on the amounts of an element present, while the ratios between the signals from various elemental nuclei scatterers indicate the chemical composition of the substance. The system is optimized for explosives by its choice of energy.

The back-scattered neutron energy is measured by a large array of detectors using the neutrons' "time of flight" (i.e., the time of arrival of the neutron allows the device to infer the velocity, which is simply related to its energy). The measured energy spectrum then produces characteristic peaks for the specific elemental nuclei. From a knowledge of the elastic back-scatter cross sections at a given energy and the relative height of the peaks, the ratios of the elements are determined. Explosives have unique ratios among their carbon, nitrogen, and oxygen quantities. These are signatures" by which they can be distinguished from other materials. Access from only one side is needed to carry out the examination.

In NRES, the incident neutron energy is varied first to excite a resonance peak due to nitrogen, and then to a nonresonant energy. Both energies are in a region where there are no resonances for either carbon or oxygen. The use of a resonant technique to highlight the signals from nitrogen while retaining carbon and oxygen signals has been demonstrated. Two complementary and simultaneous techniques would then be used to identify target elements; in combination, high detection probabilities and low false-alarm rates may be feasible.

The system has some limited capability of separating signals from different locations along the path of the neutrons. Signals from different depths will produce smearing of the time-of-flight spectrum. Time-gating of the arriving neutrons should produce depth measurements as well as sharpen the spectrum. The ability to separate these signals has yet to be established experimentally, but PENETRON claims that analysis shows that separation should be achievable.

[9] In the related medical technique of positron emission tomography, resolutions on the order of millimeters are achieved. In the case of explosive detection in baggage using the proposed system, thick NaI crystal detectors, which limit spatial resolution, will be needed for high efficiency.

[10] The developers propose to couple this technique with an x-ray system that would give a second resolved image to aid in distinguishing between nitrogen and the sources of background.

Laboratory measurements have been made utilizing a Van de Graaff accelerator at the University of Kentucky, with typical materials characteristic of explosives, narcotics, and several common materials indicating promising results. A definitive proof-of-concept demonstration requires the use of a dedicated facility.

Status

Promising laboratory experiments have been performed to verify the proposed scheme. A proof-of-concept program is needed to determine the difficulty of making the required measurements in a realistic material, in which different substances are mixed. This concept uses relatively low-energy neutrons and, consequently, the shielding requirement would be moderate. The accelerator technology also appears to be within sight. It is claimed that this technology should be amenable to extrapolation to the large cargo container problem encountered in freight hauling.

This concept is covered by several patents issued to Dr. Henry Gomberg and Dr. Marcus McEllistrem. The patents are assigned to PENETRON, Inc., a joint venture of Ann Arbor Nuclear, Inc. and the Environmental Research Institute of Michigan.

Appendix B
X-Ray-Based Detection Systems

Standard X-Ray Scanners

Sponsor: **Commercially developed and available from several vendors, such as EG&G Astrophysics, Siemens-Heimann, and American Science & Engineering (AS&E).**

Status: **In serial production, both domestically and abroad.**

Funding: **Developed through private funding. Unit cost approximately $20,000 to $40,000.**

Basic Operating Principles

The standard airport hand-baggage scanner has a fan-shaped or scanning x-ray beam that is transmitted through the object to be inspected. The absorption of x-rays is usually measured by a line of detectors, and a high-resolution image, derived from the degree of absorption of the beam, is produced. The image depends primarily on the density of objects located in the bag along the beam of the x-ray. These devices cannot distinguish between a thin sheet of a strong absorber, such as a metal, and a thick slab of a weak absorber. Simple x-ray systems rely on humans to serve as pattern recognition devices; in the absence of advanced computer pattern recognition techniques, they are very dependent on human factors, i.e., the training and quality of the observer.

X-ray scanners come in single- or two-view versions, with the two views being orthogonal. X-ray scanners present their images in shades of gray (as many as 80 shades depending on the degree of absorption), or in "pseudo-color," where colors are used to produce an artificially enhanced visual presentation.

Dual- or Multi-energy Scanners

Sponsor: **Commercially developed by several vendors.**

Status: **Commercially available. Several vendors make such equipment, such as Siemens-Heimann, and EG&G Astrophysics.**

Funding: **Commercially developed, unit cost less than $100,000.**

Basic Operating Principles

Dual-energy systems are really two x-ray systems, whose beams are generated by sources that peak at different energies, producing two independent pictures. The higher energy view suffers less absorption. While areas of heavy elements are dark in both views, areas of light elements are darker in the lower energy view. By comparing both images, light elements such as carbon, nitrogen, and oxygen may be emphasized. In this way, it is possible to determine whether a given object is made of a light or a heavy element.

Multi-energy systems are essentially the same except that they have a single x-ray tube that transmits a broad spectrum of energies. Detectors are used to select specific energy regions. Both systems produce effectively the same result.

Technical Description

This technique cannot distinguish among the light elements (e.g., tell nitrogen from oxygen from carbon). However, it can overcome the countermeasure of hiding explosives behind an object made of a heavy element (unless enough material is present to absorb the entire beam-corresponding to approximately 8 to 10 mm of steel), which standard x-ray scanners cannot.

These devices are technically identical to simple x-ray scanners, except for the dual energy and image feature. The systems use color to separate the image into organic (light elements), inorganic (usually heavy elements), and opaque materials (a lot of heavy element matter). For instance, the EG&G E-Scan system assigns the color orange to organic materials, which might include explosives. Some proponents believe that this use of color is a big help to an operator's ability to detect explosives.

Backscatter X-Rays

Sponsor: **Commercially developed by AS&E.**

Status: **Commercially available from AS&E. Computer algorithm currently under development for automatic detection of explosives.**

Funding: **The Model 1012/10122 systems are available for $60,000 to $100,000 per unit either as a single (101Z) or dual (101ZZ) view system.**

Basic Operating Principle

The AS&E backscatter system scans a pencil beam of x-rays across the object and makes two images: the normal transmission image, created by a single detector on the opposite side, and a backcatter image, created by a large area detector on the side of the entering beam. A single energy x-ray beam is utilized. A two-sided version of this system with two identical x-ray beam systems makes backscatter measurements from opposite sides of the object to enhance the backscatter penetration capability of the system.

The transmitted beam provides a typical x-ray image showing primarily the absorption by heavy elements. The backscatter signal intensity depends on how much of the transmitted beam has been absorbed, how much is backscattered, and how many of the backscattered x-rays reach the backscatter detectors. The backscatter signal depends on the competition between photoelectric absorption and Compton scattering. The photoelectric cross section increases with the atomic number of the object z, while the Compton cross section is relatively independent of atomic number. Therefore, the resulting backscatter signal favors the low Z elements, with particular emphasis on low Z elements of high density, such as plastic explosives. Backscatter imaging provides a direct measure of the density of elements with low atomic number.

Technical Description

The AS&E system produces two independent x-ray images: an x-ray transmission image emphasizing the high Z elements, and an x-ray backscatter image emphasizing the low Z elements. The system utilizes a proprietary Flying Spot technique, which sweeps a small pencil beam of x rays across the object to generate each line of image data.

A single large solid-state. transmission detector measures the x-ray absorption by integrating the detected x-ray flux over time. The Flying Spot scanning beam technology is required for efficient scatter imaging. Because only one small area is illuminated by the pencil beam at any instant of time, all detectable backscatter must come from that pixel. A large solid-state detector measures the backscattered x-ray signal, again with time integration of the detected backscattered flux. By comparing the two images, the operator can make judgments about the composition of regions of high density, which may help detect and identify threatening contents of a bag.

Currently, AS&E is implementing a computer algorithm for automatic detection of explosives with the aim of achieving a high probability of detection and a low false alarm rate for explosives. The automatic detection scheme is based on an algorithm that compares properties of object bag images against acceptable thresholds. The system builds a database of acceptable histograms by observing and "learning" the characteristics of a large variety of bags. An algorithm sorts and combines the data for online comparison with acceptable values. The AS&E system "learns" the characteristics of bags in a manner similar to the learning part of the TNA system.

Potential and Shortcomings

Implementation of the automatic detection algorithm has proceeded slowly in the past, supported only by company funding. However, the FAA has recently funded the completion of development and initial field testing of this system. Field testing is scheduled to begin within a few months. Although the automatic detection of simulated explosives has been demonstrated, to date there have been no definitive field tests of the effectiveness of the system. If this scheme is successful, it will be easy to retrofit to existing AS&E systems. The company states it can produce these systems at a rate of about 200 to 300 per year.

Computerized Tomography (CT) X-Ray Scanners

Sponsor: Commercial development with some support from the Army and FAA

Status: Pre-prototype system demonstrated by Imatron, Inc. to FAA in June 1989; Imatron claims a prototype is being readied for airport testing in the near future.

Funding: The cost of these systems will probably be of the order of $500,000 to $600,000.

Basic Operating Principles

This system is an adaptation of a compact, fast, mobile medical CT scanner, which Imatron has developed for the U.S. Amy. This concept utilizes a conventional x-ray scan projection to locate areas with sufficient density to represent a threat. In addition, multiple detectors, placed on a rotating circumferential element around the object, measure the transmitted signal from a fan beam that traverses it (as in standard CT devices). The density at each location along the path of the beam can be determined, with the rotating action giving the information to provide a complete two-dimensional slice. The inspected object is moved through the detector/beam station by means of a conveyor belt, providing the third dimension, i.e., multiple slices, for an image that then can be viewed from all angles by computer projection techniques. This technique also has very good spatial resolution (a few millimeters).

Technical Description

This system operates and looks very much like the medical CAT (computerized axial tomograpy) scanner from which it was developed. Imatron's niche in the medical CAT scan business is the field of very fast scanners, as well as portable systems designed for army field use. The explosive detection device was adapted from this work.

The system first produces an x-ray scan similar to the conventional airport x-ray scanner. An automated inspection algorithm determines the locations within the baggage where the absorption indicates a suspicious area; cross-section CT slices then need to be made to determine the density, texture, mass and shape of the object. Dual-energy CT, a theoretically possible, although not yet implemented option, would also provide information on atomic number. If no high-density areas are detected, a single slice through the bag is made to look for any sheet explosives that may not have been seen in the projection scan. Since the CT scan produces true cross section slices, it is able to identify objects that are surrounded by other materials or hidden by innocuous objects. When alarms are encountered, the CT Scan operator can make further slices to reveal size, shape, mass and make-up of the suspect object. Three dimensional rendering may also be applied.

The Imatron CTX 5000 uses color coding to highlight possible explosives. The spatial resolution may be good enough to locate wires, detonators, or related bomb components.

Potential and Shortcomings

The current claim for throughput is 360 bags/hour, which is too slow for current FAA requirements. This throughput is calculated assuming an average of 2.5 slices per bag. Only field experience can establish what the real requirements will be. Since this limit derives from limits on speed of computation, it is possible that future computer improvements (which are coming very rapidly) will sufficiently increase the speed of the system. The current aperture diameter is 63 cm, which is too small for some bags. Future versions will have an 80-cm diameter aperture, according to the vendor. The ability to resolve explosives using only density information was investigated at LAX by CT scans of 900 checked bags and 100 bags with simulated explosives in a FAA sponsored test in 1988. The results were encouraging to the vendor. However, more precise data, including detection probabilities, false alarm rates, and throughput will have to be determined through more extensive tests. Unit cost is estimated by the vendor to be around $500,000 to $600,000.

Vapor Detection Systems

Gas Chromatography With Chemiluminescence

Sponsor: Federal Aviation Administration (FAA) Technical Center; Department of State; both supporting contracts with Thermedics, Inc.

Status: Hand-held unit is in production for U.S. Department of State and other buyers. Prototype for "walk-in" style of detector for airport concourse security is being built for FAA but is not yet formally tested.

Funding: Approximately $7 million from the Department of State since 1985 and approximately $5 million from the FAA since 1984, plus some private funding ($6 million) from Thermo Electron Corp., the parent of Thermedics.

Basic Operating Principle and Goals of Concept

These devices use gas chromatography, a fully mature technology, to separate a sample of molecules from a carrier gas and to isolate molecules of different chemical compounds from each other. The sample is taken with a portable hand-held collection unit that heats up the sampled surface with infrared lamps and sucks air from near the surface.[1] Heating is important, since vapor pressure increases by a factor of 10 for every increase of 10 ‘c.

The sample is then injected into chromatographic columns, which consist of thin tubes lined with a material that absorbs or dissolves the molecules of interest, thereby retarding their passage through the column. Different molecules are slowed to different degrees. The material with the least affinity for the column substrate will go through fastest and those with increasing affinity will traverse the column in longer times. Residence time within the column can be adjusted by varying such factors as column length and temperature. Furthermore, since different materials are released from the column at different times, this technique allows mixtures of material to be resolved. With proper calibration, the residence time of a given type of molecule within a given column is predictable and can be used to identify the molecule.

At the termination of the separation process, column contents are heated to pyrolyze the explosive compounds into fragments, among them nitric oxide (NO). The chemiluminescent reaction of nitric oxide with ozone (O_3) is well known[2] and yields photons that can be detected by conventional means[3]. This signal is analyzed by a microprocessor to determine if it meets predetermined criteria for alarm. The timing of photon detection can be used to identify those explosive compounds present, since each compound has a characteristic speed of migration through the column.

While this strategy relies on familiar instruments and well-known chemical reactions, it is by no means an insignificant task to perfect the operational parameters so that minute quantities of material can be successfully and reliably recognized within a few seconds. Through a proprietary combination of column lengths and temperature cycles, the manufacturer of this device, Thermedics Inc. of Woburn, MA, claims to be able to detect plastic explosives rapidly. Independent tests have also shown that the device has this capability. The company also ran tests that appear to show that their walk-in booth, based on the same technology, responds to plastic explosives hidden under one layer of clothing.

Technical Description

The only difference between the hand-held and walk-in models is the sample collection step. In the walk-in device, an individual to be tested stands in a booth where air is vigorously blowing. The velocity of the air is sufficient to cause at least the outer layer of clothing to be agitated. Simultaneously, the subject's skin and clothing are warmed by infrared heaters. This facilitates the escape of any target molecules. The air currents are collected through a series of funnels positioned in a vertical array in the back of the booth.

The hand-held device consists of two units: a testing unit and a collector. The testing unit is about the size of a 55-gallon drum and contains the chromatographic columns, chemiluminescent reaction chamber, and all the display instrumentation. The collector, which is about the size of a large hand-held vacuum cleaner, contains a suction device and is adapted to be placed against or near an object to be tested. The head of the collector unit includes a heat source and appropriate ducting to direct the resulting air stream onto a preconcentrator. This unit consists of a high surface area substrate made of a material onto which active molecules (which would include any explosives) in the air stream attach themselves while inert materials are blown past. At appropriate intervals, mole-

[1] The walk-in portal unit samples quite differently and is discussed separately. Except for the sampling, the two units are essentially the sine.

[2] P.N. Clough and BA. Thrush, "Mechanism of Chemiluminescent Reaction Between Nitric Oxide and Ozone," *Trans. Faraday Soc., 63,915 (1967).*

[3] See U.S. Patent No. 3,763,877 issued Oct. 9, 1973 entitled "Fluid Flow Control System."

292-884 0 - 91 -- 4 : QL 3

cules are released by warming the preconcentrating device. For the hand-held device, this operation is performed after the device has been clamped into the testing unit.

The expelled gases pass through a series of chromatographic columns specially designed to facilitate separation of the target molecules from the carrier gas and from each other. The chemiluminescent reaction is performed on the columns' effluents. Lights on the operator's panel indicate which, if any, explosive has been sensed. A more informative display is also available in the form of a video monitor, which shows the chromatogram (a chart on which the time of arrival for each compound appears as a peak) as well as a hard copy from a thermal printer.

Potential and Shortcomings

Opinions on the merits of this device vary considerably with the customer. This device is one of the few sniffers on the market that claims to be able to detect pure plastic explosives. In a maintenance-plagued test of a prototype device conducted on real luggage in February 1989, the FAA reported that the hand-held system did not perform well.[4] However, more recent tests, both in the United States and abroad, including some in an airport environment, have produced far better results. Further FAA testing has been done, but the results have not yet been released.

The experience of the State Department has been far more positive. The State Department was interested in a different set of criteria than was the FAA. High throughput was not as important in the State Department's application as it is in an airport environment. State was also willing to accept a higher percentage of false positives because the inconveniences associated with such readings were less serious for their purposes. They wanted a device that could be easily operated by technically unsophisticated foreign nationals. For these reasons they were attracted to the Thermedics products. Tests conducted for the State Department showed certain maintenance problems (apparently resolved now) but confirmed the sensitivity of the device to plastic explosives and concluded that the device had promise. One foreign country, investigating this device for purposes and using methods not originally envisioned by the manufacturer, has reported very favorably on its performance. In December of 1989, they were given the use of a Thermedics machine for a few weeks and they proceeded to try it out in every possible environment: airports, harbors, border crossings, and post-blast forensic work. They were impressed with the machine's ability (unique, in their opinion, among the "sniffers" they had tested) to respond accurately to the plastic explosives. They found the machine insufficiently rugged, in its current state of engineering, and too slow to operate effectively in a high throughput situation such as the baggage area of an airport. However, significant improvements have recently been achieved and field testing within the past year has shown far superior performance with respect to maintenance and operation. The ability of this device to identify an explosive was superior to that of other analytical techniques now used. Several other countries have also tested this device, and a number of foreign sales have been made, some for airport use.

The hand-held device is in commercial production and sells for about $150,000 (including an extra chemistry module) under the tradename EGIS II.

The device operates remarkably quickly for a gas chromatography. The gas traverses the chromatographic column very quickly and subsequent signal analysis can be completed in about 30 seconds. Some customers find this speed acceptable, but current performance of the walk-in booth (due to slow sample collection time) would not meet FAA concourse throughput requirements unless several units were operated in parallel, or a completely independent prescreening technique were used, or unless several individuals were scanned at the same time. Because it is capable of identifying which explosive compound has been detected, this system is very useful for post-blast forensic investigations. Some tests have also shown an increased effectiveness using the wipe-down technique: wiping a suspect objector person with a paper cloth, and then sampling the cloth.

Information on the current sensitivity of this device to interferants and false alarms was not available, although tests on earlier units found false alarms due to local contamination to be a problem. The manufacturer asserts that the current production devices have very low susceptibility to interferants. Another problem might be that the chemiluminescent reaction is reported to be not particularly sensitive. However, the sampling and collection of these machines is very efficient. Furthermore, the technique is quite selective relative to other vapor detection techniques, allowing the detector to operate at sensitivities that appear to be competitive with these other methods.

[4] The manufacturer claims that this test is not representative Of the performance of this device and that the current model performs better. Further, some problems were claimed, also by the manufacturer, to be due to cross-contamination in the FAA's laboratory rather than to the machine's performance.

Gas Chromatography With Electron Capture Detector (GC/ECD)

Sponsor: FAA
U.S. Navy
Canadian Government (for development work by Canadian firms)

Status: Workable machines are in production by several manufacturers; R&D is being done to improve selectivity and trapping, to expand the range of explosives to which the device is sensitive, and to develop improved walk-through device.

Funding: About $1 million over the last 3 years.

Basic Operating Principles and Goals of Concept

This equipment tests for low volatility, high electronegativity substances. Like the chemiluminescence device described above, these machines also make use of a chromatographic column as a first step to physically separate explosive molecules from other components of a gas stream. The detector, however, is quite different. A small radioactive source ionizes a gas mixture to form free electrons that flow towards an anode, thereby creating a constant current. Molecules emerging from the column are mixed with these electrons. Being quite electronegative, the explosive molecules will "grab" some of the electrons. Fewer electrons will then be available to flow towards the anode, and this effect is sensed as a decrease in the current. Microprocessors analyze this change to determine if it meets predetermined criteria for an alarm.

Several configurations of this detection strategy are commercially available and have found wide use throughout the world.

Technical Description

In a typical electron capture device--for instance, the Ion Track Instruments Model 97—an air sample is aspirated into the detector and impinges on a membrane. Air and many contaminants (most critically, oxygen, halogens, and water vapor, which would foul up the detector downstream) are thereby separated from the molecules of interest, which diffuse across the membrane into a stream of argon gas. This stream is then directed into a pair of chromatographic columns. This device, however, uses two parallel GC columns, one coated with a chromatographic substrate known to retard polar (electronegative) materials such as explosives compounds and the other coated with a nonpolar substrate.

In the electron capture detector, the effluent from each of the chromatographic columns-which contains argon gas—is piped into one of a pair of detectors where it is irradiated with beta particles from a small radioactive source to yield a plasma containing Ar^+ and electrons. The electrons flow towards an anode, creating a measurable current. If highly electronegative explosive molecules are present, they will combine with some of the electrons to form negative anions, thereby depleting the available stock of electrons. This depletion is manifested as a decrease in current. If there is no change in current, or if a change occurs simultaneously in both detectors, no alarm is sounded. However, if a substance is delayed by the polar chromatographic column, the detector attached to this column will react later than the detector from the nonpolar column. If this delay occurs within a preset time window (typically 10 milliseconds or so) and other signal criteria (that vary with equipment design) are met, an alarm occurs.

Other manufacturers employ variations of this strategy. For example, a wad of adsorbent material maybe used in place of the membrane to separate sample molecules from the air stream. Another variation uses a single GC column attached to a single ECD. A microprocessor decides whether the timing and other characteristics of the signal are indicative of the presence of an explosive. The Canadian firm, Scintrex, is now marketing a dual-column device; one column is designed to respond to the EGDN-based explosives and the other to the NG/DNT group.

These devices are available either as hand-held units or as walk-through models. For example, the hand-held ITT Model 97 has been on the market since 1978 and currently costs about $15,000. The walk-through version of this device is sold by ITT under the tradename EntryScan for about $30,000. Other GC/ECD products include the EVD-1 manufactured by Scintrex (selling price for the dual column model, widely acclaimed for its ability to sense EGDN reliably, is about $45,000) and Scanex Jr. from Sentex Sensing Technology of Ridgefield, NJ.

Potential and Shortcomings

The commercial models of these devices were among those tested by the FBI in their 1988 experiments. In general, they all sensed the higher vapor pressure compounds but were unable to detect the plastics and other very low volatility materials.

While ITI claims to have detected SEMTEX with their Model 97 device, most observers feel that the device was actually responding to a contaminant (which does not appear to be reliably present in the material) rather than to the explosive itself. ITI asserts that all SEMTEX tested on the detector has shown presence of contaminants, which it states are unavoidable residues from the manufacturing process. Not all experts agree, however. ITI also claims sensitivity to Detasheet (although their detector, like the other units tested by the FBI, failed to respond consistently to this material under field conditions) and, to some degree, to U.S.-manufactured C-4. ITI claims that an upgraded version has improved detection capability for plastic high explosives.

In the FBI test, vulnerability to interferants varied among the detectors and apparently was related to the fine points of the preconcentration and signal processing subsystems. In the field, maintenance remains a problem. Apparently the need to deal with an inert gas bottle, a characteristic of all ECD devices, has been a problem, as has fouling by airborne particulate matter. The response time of some of these devices can be fairly slow (on the order of minutes) although others, such as the ITI 97, have a response time of less that 2 seconds. Some require a prolonged (i.e., 20 minutes) warm-up time.

Current work is aimed at improving trapping techniques to be used upstream of the ECD. In work performed for the U.S. Navy, ITI has experimented with a batch mode of operation in which the membrane is kept at a low temperature, under which conditions it functions not just as a separator but also as a preconcentrator. Recent tests of this device show promise.

Other experimental work is aimed at developing a so-called rotary trap. This is a constantly rotating, circular plate having a glassy adsorption layer. Sample air is drawn through the plate at one location. At a second location, the plate is heated to release the entrapped molecules. Additional work is being done to improve a walk-through version of this device.

Ion Mobility Spectrometry (IMS)

Sponsor: Technology is commercially available. Some work is being sponsored by the FBI and by the Canadian government.

Status: Commercially available under the Graseby trademark; marketed in the United States by Astrophysics Research Corp. of Long Beach, CA (now, EG&G Astrophysics). Similar technology is used in units marketed by Barringer, Inc. of Canada, through its U.S. subsidiary.

Funding: About $100,000 over fiscal years 1989 and 1990.

Basic Operating Principles and Goals of Concept

Air containing vapor or a stream of airborne particles from an area to be tested is drawn in through a sampling probe. Air and explosive molecules diffuse through a membrane or a filter into a chamber where a sealed ^{63}Ni radioactive source ionizes the sample. Periodically (about 50 times per second), small bursts of ions are released into a separation region by an electronic gating grid. Under the influence of an electric field, these ions move down a drift tube against the flow of a separation gas. The speed with which these ions move through the tube is a function of their mass, their charge, their physical shape, and the amount of diffusion (deviation from a straight-line path). Heavier ions, such as those of explosives compounds, tend to travel more slowly than lighter, simpler ones typical of air. The drift region terminates in a collector electrode. Ions reaching this collector will cause a small current peak. The position (in time) and magnitude of this peak are analyzed by a microprocessor in order to determine the identity and concentration of the vapor being detected.

Potential and Shortcomings

In the course of the FBI test, this device operated with about the same reliability and sensitivity as the other vapor detectors examined (which were all GC/ECD devices). The machine was able to detect the higher vapor pressure explosives, nitroglycerine and DNT, but did not respond to the lower vapor pressure materials such as TNT or RDX. It was slightly more susceptible to false alarm than the other devices. Like the others, it was unable to reliably detect explosive threats in simulated real life situations.

FAA sources note that these machines operate at thermal equilibrium: the ions created by the radioactive source stay close enough together for along enough time to allow numerous molecule-molecule interactions. This can cause scrambling, whereby the ionized explosive molecules collide with other molecules and in so doing, give up their extra electrons. Such de-ionized particles would not be sensed by the machine. Also, due to the duty cycle of the grid, 99.9 percent or more of the explosive molecules never reach the detector. Given initial quantities of materials in the pico- or femtogram range, such losses can be devastating to sensitivity. Finally, even the sales literature for these machines indicates that accuracy is dependent on the training of the operator.

On the plus side, however, several groups see promise in an improved version of this device. Work at Sandia National Laboratory has established that under ideal conditions an IMS detector can find plastic explosives, being sensitive to as little as 30 femtograms of explosive, despite the built-in 10^3 to 10^4 losses caused by the duty cycle of the g-rid. Other groups from Washington State University and New Mexico State University are also working on perfecting operating parameters for this device. While most of this work is aimed at detecting trace environmental pollutants, the results are easily applicable to explosives detection.

Further, quite recently, the Canadian firm Barringer has claimed that its IMS machine can reliably detect plastic explosives by adapting the device to collect and process particles (as opposed to vapors). At least one set of independent confirmatory tests has been made at Picatinny Arsenal, U.S. Army. The device has also been tested in November 1990 by the FAA. Results have not yet been publicly released. While this machine has been demonstrated in the laboratory and for other purposes (notably narcotics detection), field operability for explosives detection still needs to be determined.

Two Stage Mass Spectrometry (MS/MS—Low Pressure Glow Discharge Ionization)

Sponsor: Department of Energy, work being done at Oak Ridge National Laboratory (ORNL), Oak Ridge, TN.

Status: First generation system operational. Theoretical work on second generation device nearly completed. ORNL wishes to transfer technology to industry for development.

Funding: Funded by the Department of Energy since fiscal year 1984. Funding level was about $400,000 in fiscal year 1990. About the same amount or slightly less for each of the three previous years.

Basic Operating Principles and Goals of Concept

Each mass spectrometry stage makes use of the fact that many explosive molecules are nearly unique among natural compounds in their electronegativity, that is, their propensity to attract and capture an extra electron and thereby become negative ions. Once ionized, they can be accelerated and analyzed by subjecting them to electric and/or magnetic fields. The mass-to-charge ratios of the ions can be determined by any of a variety of means referred to collectively as mass spectrometry.

In the MS/MS explosives sniffer developed at ORNL, an air sample is drawn through a small orifice into a low-pressure chamber where an electric current flows through the sample and ionizes molecules of air and, especially, of explosives, if present. This process is called air sampling/glow discharge ionization (ASGDI). Due to various inefficiencies and the contrary properties of explosives molecules, the negative ions from the ASGDI chamber that are injected into the first stage mass spectrometer will include only 1 to 5 percent of the explosives molecules originally drawn into the chamber.

By capturing the output of the first stage mass spectrometer at a given time after injection or at a predetermined spatial location, usually a slit, the ions with particular mass-to-charge ratios are separated from the complex mixture.

Large molecules, such as the explosive compounds, can be fragmented into predictable smaller pieces. The output of the first stage is brought into collision with a stream of neutral atoms such as helium. The impacts cause the large molecules to dissociate into smaller ions, the masses of which can be determined by a second mass spectrometer. Because it is unlikely that more than one kind of molecule will both ionize to the proper mass-to-charge ratio *and* break down into the proper fragments, this technique is considered to be very specific in detecting explosive materials and thus yields a very low false alarm rate.

Technical Description

An air sample is preconcentrated and drawn into the analysis device. optimization of these preliminary steps has not been a focus of the researchers at ORNL. Molecules in the sample are ionized at low pressure (approximately 0.8 torr) in a novel glow discharge chamber.[5] By operating at low pressure and in short time frames, they were able to avoid ion/molecule reactions involving analyte ions that could cause the analyte ions to transfer charges to background molecules, thereby eliminating or altering the signal.

The ions thus generated are then passed through a quadruple mass filter: four parallel cylindrical rods that create an electrical field pattern that effectively screens out all ions except those of particular predetermined mass-to-charge ratio. The mass-selected ions are then broken into fragments by collision with helium gas. The masses of the ionic fragments are then determined using a time-of-flight spectrometer. In time-of-flight spectrometers, the ions are accelerated by applied electric fields and sent through a flight tube. Ions of different masses pass through the flight tube at different speeds.

In a second-generation device, both quadruple mass filters and the time-of-flight instrument have been replaced with an ion-trap mass spectrometer (ITMS).[6] This change promises to provide a smaller, more specific, and sturdier mass analyzer. The researchers at ORNL are currently working on perfecting techniques for injecting ions into the ITMS.

Potential and Shortcomings

This device was evaluated by Sandia National Laboratories in August 1988.[7] It was found to be very insensitive to interferants, even those suspected of being able to disturb the glow discharge chemistry on which the ionization of the first stage depends. The device was able to respond accurately to samples of RDX, C-4, military TNT, tetryl, the cut end of a sample of Primacord, and Detasheet, although it should be noted that the test

[5] See U.S. patent No. 4,849,628 issued July 18, 1989.

[6] Scott A. McLuckey, Gary L. Glish, and Keiji G. Asano, "Coupling of an Atmospheric-Sampling Ion Source with an Ion-Trap Mass Speetrometer," *Analytica Chimica Acta 225 (1989) 25-35.*

[7] F.J. Conrad and D.W. Hannum, "Evaluation of the Oak Ridge MS/MS Explosives Detector," pp. 35-1 to 35-17, Sandia National Laboratories, 1988.

protocol involved near contact with the explosive sample.[8] Under these conditions, the device was sensitive to concentrations of explosive molecules in the range of 0.3 to 30 parts per trillion and to quantities on the order of 50-100 femtograms. No problems with maintenance or reliability were reported after the ion source had run for months at a time without breakdown or need for cleaning. Prototype versions of this arrangement have been used at ORNL. Licensing agreements have been reached with a private corporation that has plans to market a similar device as an environmental monitor and is evaluating the market for explosives detection.

Fluoroimmunoassay (Antigen-Antibody Reactions as a Test Technique)

Sponsor: FAA Technical Center; work performed at Naval Research Laboratory (NRL)

Status: Beyond Proof-of-Principle. Awaiting practical testing later this year.

Funding: $250,000 per year.

Basic Operating Principles and Goals of Concept

A continuous flow of vapor to be tested is drawn into a preconcentrator at a rate of about 2,000 liters per minute and collected in 1 ml of aqueous solvent. The output of the preconcentrator is directed into the detection unit. This unit is a small (200 microliter) vial containing immobilized antibodies and fluorescently labeled analogs of explosive molecules. The antibody reacts with extreme specificity to only one particular explosive. If present in the sample, the explosive antigen will displace its fluorescently labeled analog, which can be easily detected downstream.

Technical Description

The test takes about 1 minute. To minimize false alarms, two columns can be used in parallel, with the second column containing an irrelevant antibody/fluorphore-labeled molecule pair. Any substance that causes an alarm from both columns is obviously not reacting with the antibody but is releasing fluorescent material by another pathway. Antibodies to more than one explosive can be used simultaneously.

Other workers in this field (Westinghouse and Biometrics, Inc.) are also using antibodies to test for the presence of explosives but use a capacitive device instead of fluorescent labeling for detection.

Potential and Shortcomings

Field tests are scheduled to be conducted in the near future. However, some performance characteristics can be inferred from antibody detector work in other areas. The detector is fairly inexpensive, fast, and fully automated. Because each antibody is specific to a single compound, a detection unit would need to contain antibodies to all materials expected to be encountered. Researchers at NRL claim that their device is sensitive to nanogram (10^{-9} g) quantities of material. This is substantially less sensitive than many other of the technologies discussed above. However, the investigators are now working on coupling a preconcentrator onto the front end of their device. This technique is said to be able to convert a vapor sample containing 10 ppt TNT into a 5 microliter solution, which is easily detected by their machine.

[8] If the device failed to alarm under these conditions, a preconcentrator (such as a wad of quartz wool held near the explosive sample over which an air stream was drawn) was employed.

[9] Finnigan-Mat Corp., San Jose, CA.

Appendix D

Chemical and Biological Warfare Agent Detection

This appendix summarizes work done in detection of chemical and biological agents in recent fiscal years.

Biochemical Detector System

Sponsor: U.S. Army-Chemical Research, Development, and Engineering Center (CRDEC).

Status: Exploratory development of an automated Army field device.

Funding: Approximately $5 million per year.

Basic Operating Principles and Goals of Concept

This system is a "simple" point detection alarm that classifies and partly quantifies nerve and blister gases as well as pathogens and toxin agents. Detection is accomplished at levels consistent with human sensitivity to the agents. The device is to operate unattended and continuously. The system consists of an aerosol sampling subsystem, a sample preprocessor, and a detector.

Technical Description

This device is designed to be a 10-pound, l-cubic-foot object that operates continuously when unattended. A cassette feeds film through the sample stream drawn in by the aerosol sampling subsystem (a suction pump). In the preprocessor, antibodies from a storage system are directed towards the sample where they attach to any antigens that are present. The agglomerate sticks to the film at specific locations. The antibody has an attached radical that increases the acidity of a solution in which it is dissolved. If the antibody/antigen combination is present, the pH of the spot will then drop, due to the increased acidity, indicating the presence of the agent. The pH is measured indirectly through a simple measurement of the conductivity of the spot.

Status

This is a major Army development program designed to bring chemical and biological weapon (CBW) detection capability to field use, and is not directly aimed at the terrorist threat. The program is currently in exploratory development. The engineering development phase is slated to start in fiscal year 1993. Technology from this program could be utilized to produce some near-term, terrorist-specific hardware, which would not necessarily have the same degree of automation or the same weight specifications but might have the need for a more rapid response.

Potential and Shortcomings

This point detector is a local measuring device with a limited range. It responds only to those specific agents that it is designed to search for. This is a general weakness of all detection and analysis schemes that utilize anitbodies. Such systems are primarily useful when an attack by a specific set of agents is suspected.

Chemical and Biological Mass Spectrometer

Sponsor: U.S. Army-CRDEC

Status: Exploratory development—technology base studies.

Funding: $8.8 million through fiscal year 1990-$30 million projected through to production and deployment.

Basic Operating Principles and Goals of Concept

This device is a somewhat more sophisticated automated point detection system designed to detect, identify, and semiquantify chemical and biological materials in an air sample. It is designed to detect known chemical agents, toxins, and pathogens that are listed in an internal library.

In later versions, it is hoped that the device will be able to identify unknown agents based on stored characteristics and expert system software (i.e., software that allows the system to employ programmed methodologies, assembled from human pathologists, that are intended to evaluate an unknown threat).

Technical Description

This instrument is a major extension of an existing German mass spectrometer instrument, which can perform a limited detection and identification function. The specified improvements over the existing device include a quicker response time, a broader range of observable materials, increased resolution (i.e., ability to identify), a larger library of agents in the data bank, and reduced physical weight, size, and power requirements. This system is designed around a two-stage mass spectrometer for detection and identification. It consists of a biosampler unit, an infrared pyrolyzer that prepares the sample, and the mass spectrometer itself. The device is designed to weigh 40 pounds and have a volume of 2 cubic feet.

Status

This is a long-range development program for the Army, currently in the exploratory development phase. A simpler and more modest version of this technology, possibly based on the German system, could be of some value to the terrorist detection problem and could be available at a much earlier date than the current Army program.

Potential and Shortcomings

Like other chemical and biological detection and identification concepts, this system depends on stored data on potentially harmful agents that are known to exist. The use of artificial intelligence techniques for implementing the process of identifying unknowns is in an early stage of research and its success cannot yet be forecast.

* * *

The following are smaller projects, sponsored by the Technical Support Working Group (TSWG) and conducted by various laboratories and contractors under the technical and contractual supervision of the Naval Explosive Ordnance Disposal Technology Center at Indian Head, MD. In general, these programs do not develop brand new technology, but are applications of existing capabilities *specifically to the counterterrorist problem.*

Building Air Monitor

Sponsor: TSWG—through the U.S. Army CRDEC

Status: Contractor efforts at Los Alamos National Laboratory (LANL) and at the Illinois Institute of Technology Research Institute (IITRI) during fiscal years 1988, 1989, and 1990. Systems demonstrated at CRDEC in 1989 and 1990.

Funding: *LANL—$120,000* in fiscal year 1988; $198,000 in fiscal year 1989.
IITRI--$351,000 in fiscal year 1988.

Basic Operating Principles, Goals of Concept, and Technical Description

The object of both these efforts is to develop a real-time chemical vapor and biological detection system to monitor fixed-site air supply systems. The LANL system utilizes a Zeeman interferometer that detects the change in the index of refraction of air or water when a contaminant is present. The measurement is not very sensitive or very specific, but is instantaneous. This is a major advantage for an early warning system. The IITRI program uses modified, off-the-shelf, flame photometry equipment.

In the LANL system a commercial Zeeman laser[1] shines through a reference chamber and into a photodetector. A phase shift between the two lines is measured and related to the refractive index of the medium. For a 5-centimeter path length, the refractive index can be measured to 1 part in 10^{9}. In practical terms, the sensitivity is about 1 part per million (ppm or 10^{6}) for air and gases and about 1 part per billion (ppb or 10^{9}) in water (the change in index is much greater for water). Since the only observable is the change in index of refraction, the device can only note that the baseline content of the air or water has changed. The project has been completed and a final report is nearly complete. No hardware has been delivered.

The IITRI system uses a liquid chromatography and a standard flame photometer to identify GB, VX, and DFP (nerve gases) concentrations at parts per trillion (ppt or 10^{12}) levels in a 7-minute analysis cycle. In a flame photometer, the sample is passed through a flame that excites the molecules present. These excited molecules then radiate light at characteristic frequencies, which can be used to identify the molecular species. The work on this project was initiated in fiscal year 1989 and is continuing through 1990. Demonstration of the capabilities of the system is expected at CRDEC in the near future.

Real-Time Water Monitor

Sponsor: TSWG—through CRDEC program.

Status; *Program* scheduled for completion soon. Project is being carried out with the support of the Environmental Protection Agency (EPA) by a contractor.

Funding: *$510,000 in* fiscal year 1988; $486,000 in fiscal year 1989.

Basic Operating Principles, Goals of Concept, and Technical Description

The object of this program is to develop a highly sensitive and specific monitoring device capable of measuring chemical and biological contaminants in surface and ground water supplies.

The system consists of a sampler and preconditioned module, which gathers a sample from the water supply piping. The sample is heated uniformly to a set temperature and its pH adjusted to a set level. The sample is then processed to remove excess minerals. The conditioned sample is then fed to two sample modules, one to detect chemical contaminants and one to detect pathogens.

Currently this system is partially developed and tested, with the pathogen unit lagging behind schedule. Operating and detection software are also being written and tested, with the pathogen system again behind the other.

[2]That is, the frequency can be shifted rapidly among many different lines that arise from transitions between energy levels of a multitude of rotational and vibrational states of the CO_2 molecule.

Combination Detector System

Sponsor: **TSWG—through CRDEC program.**

Status: **Demonstration of feasibility soon.**

Funding: *$521,000 in* **fiscal year 1988; $270,000 in fiscal year 1989.**

Basic Operating Principles, Goals of Concept, and Technical Description

The objective of this program is to develop an on-line air and water monitoring system for chemical (nerve) and biological agents using a laser fluorometer to detect changes in the fluorescence of a sample. The work is being undertaken at LANL. The system can detect one ppt of nerve agent and 0.1 ppt of biological protein in aerosols, with a sensitivity of about a factor of 100 lower in water. Detection times are quick.

A sampler collects either a gaseous or a liquid sample into a continuous flow system. A pulsed laser (KrF excimer laser) fluoroscope irradiates the sample. To detect nerve agents, immobilized acetylcholinesterase (the actual target of nerve agents) is exposed to the sample and is then monitored using a substrate that fluoresces under illumination by the ultraviolet (UV) laser light. A change in activity indicates the presence of a nerve agent. To detect bacterial particles, the system observes the fluorescence emitted by aromatic amino acids and proteins (usually tryptophan) when excited by the uv light. The fluorescence-based chemistry for these compounds has been developed under this program.

This system is nonspecific and is intended as a "first alarm." The hardware consists of state-of-the-art laser and other components and weighs on the order of 45 kilograms.

Remote Agent Detector

Sponsor: **TSWG—through CRDEC.**

Status: **Feasibility demonstrated in fiscal year 1990.**

Funding: **At Stanford Research Institute (SRI)—** ***$428,000 in*** **fiscal year 1988; $0 in fiscal year 1989; $405,000 in fiscal year 1990. CRDEC contributed $50,000 in fiscal year 1989.**
At LANL--$497,000 in fiscal year 1988; $450,000 in fiscal year 1989.

Basic Operating Principles, Goals of Concept, and Technical Description

Two concepts, based on different operating principles, are being pursued by two contractors (one at SRI and one at LANL). Both are lidar systems, i.e. radar-like systems using pulses of light instead of microwaves. Each operates by sending out a pulse of light and measuring the backscattered energy and time of arrival. The intensity gives some indication of the strength of the scatterer, i.e., its concentration, and the time of arrival gives the range to the backscatterer, i.e., its location. Consequently, lidar systems can map the location and concentration of a cloud containing an agent.

The SRI system uses a frequency agile,[2] pulsed, infrared (CO_2) laser operated in a differential absorption mode (DIAL). In a lidar system some light must be reflected back to the detection telescope; the source of the reflection can be a topographical object (the ground, trees, any reflector behind the cloud to be observed), or it can be the aerosol particles of the cloud itself. In either case two (at least) pulses of different wavelengths are emitted in rapid succession, one at a wavelength where the agent in the cloud absorbs and one at very nearly the same wavelength but where the agent does not absorb. The differences between the two signals can be used to determine the concentration and in some cases the location of the agent cloud.

Laser DIAL techniques for atmospheric measurements have advanced to a fairly high state of technology, using both air- and land-based mobile platforms. The SRI program is an application of the state of the art to CBW detection. The U.S. Army has an aggressive research program aimed at developing mobile (moving) detection capability with ranges out to 10 kilometers (km), with both aerosol and surface contaminant capability. The system under development for TSWG is designed for a range of only 1 km but permits automatic, unattended operation. It is closely related to much larger Army-sponsored efforts and employs very similar technology. A system demonstration is scheduled soon.

The remote agent detection system being developed by LANL is based on measuring fluorescence induced by the absorption of ultraviolet (UV) photons from a pulsed uv (KrF excimer) laser. The uv light pulses excite fluorescent radiation of amino acids in the protein of toxins or bacterial spores or cells. The measurement is not specific. A telescope detects the fluorescence and, utilizing appropriate computer software, the system determines the location and pattern of the cloud and produces a map. At present, the system has a demonstrated range of 1.2 km. The system was field tested in October 1989 to demonstrate the feasibility of the concept.

Mobile Laboratory

Sponsor: **TSWG—through CRDEC program.**

Status: **One of two modules complete in fiscal year 1989; the second to be completed in the near future, funding permitting.**

Funding: *$611,000 in* fiscal year 1988; $0 in fiscal year 1989; $645,000 in fiscal year 1990.

Principles of Operation, Goals of Program, and Technical Description

The objective of this program is to develop a fully transportable, rapid response, analytic laboratory, capable of sustained operation in a contaminated environment, to detect, identify, and quantify the spread of chemical and biological agents released by terrorists into the water or air. The program is being conducted with support from the Environmental Protection Agency (EPA) by a contractor, Engineering Computer Optecnomics (ECO), Inc.

The significant characteristic of this concept is that the lab is readily mobile, that is, it can be transported by helicopter, aircraft, truck, rail, or ship. It is designed to respond to an emergency call and be onsite and ready to function within a few hours of a decision to deploy. The laboratory is a fully self-sustained, closed ecological system; containing its own water, electricity, fuel, and waste disposal; protective gear for the operators; and airlocks for entry and egress without contamination. It is designed as a positive over-pressure air system with intake air filtration. It has analytic capability for both chemical and biological agents, including a gas chromatograph, a mass spectrometer, various chemical agent test kits, immunologic test equipment, and sample culture apparatus. It also contains a modified glove box with sample pass-through arrangements and decontamination capability.

The analytic laboratory (an 8 x 20 foot van module) has been completed. A coupled unit containing living quarters has been designed but not completed due to a lack of funding in fiscal year 1989. It is scheduled for completion soon.

Improved Expedient Hood

Sponsor: TSWG--through CRDEC,

Status: Prototypes available.

Funding: $122,000 in fiscal year 1989.

General Principles of Operation

The objective of this program is to develop a low-cost, disposable, limited-time-duration (5 to 15 minutes), ocular and respiratory protection system for key human beings in case of an unexpected terrorist attack using chemical or biological agents. The device is simply a hood with an integral breathing apparatus (with an activated charcoal filter) and an air seal at the neck, which provides a temporary, lightweight, sealed environment for the wearer.

This development is an upgrade of current chemical agent protective gear to make it lighter, easier to store, and cheaper to manufacture. Its chief advantage is that it is a very small package that will enable potential targets, or their guards, to carry it easily for rapid use. The program will test various designs that have been fabricated in fiscal year 1990 and select a final design for future acquisition.

Appendix E

Recent Federal Counterterrorism Research Efforts: Agencies and Their Budgets

Summary

This appendix consists of a catalog of Federal agencies currently exploring new technologies applicable to the fight against terrorism. It begins with a review of the budgets devoted to these efforts in some recent fiscal years. A brief description of the direction each agency has taken in research efforts is also provided.

The largest expenditure of research funds (almost $200 million per year) described is made by the Department of Defense (DoD). The Army has budgeted about $165 million per year to support development of a wide array of technologies, from protection against chemical and biological assault, to explosives detection, to physical security and site protection. Nearly all of this effort is directed towards the support of battlefield objectives, including the area of low-intensity conflict. But some items may also be applicable to counterterrorism.

In the specific area of combating terrorism, the military services have budgeted some $16 million in fiscal year 1990 for R&D. Further, the Defense Nuclear Agency bears primary responsibility for protecting the Nation's nuclear weapons stockpile and has been working on improving means to detect and deter intruders (about $5 million per year). Another DoD agency, the Defense Advanced Research Projects Agency (DARPA), has just begun to direct its attention to the threats posed by terrorism and has budgeted about $5 million this year for research into this field. Some other DoD components have smaller efforts.

Most other Federal agencies spend much less than DoD. The Federal Aviation Administration (FAA) runs second to Defense in yearly expenditures (among the agencies that gave OTA information). The FAA Technical Center in Atlantic City, NJ spent about $13 million in fiscal year 1990 and is planning to spend about twice that much in fiscal year 1991 to develop enhanced security measures for commercial aviation. The Department of State, whose overseas facilities have frequently been the target of terrorist activities, is supporting research into a variety of security measures including explosives detection, site hardening and intrusion detection, and countermeasures. Over the last 4 years, State has invested about $7 million in this effort. State also leads the Technical Support Working Group, a unique interagency effort to recognize and support promising research and development in counterterrorist measures not adequately supported by any other agency.

In fiscal year 1989, the Department of Energy spent about $6 million researching new technologies, primarily in connection with their nuclear safeguards and security programs. Within the Treasury Department, the U.S. Customs Service has recently devoted about $5 million per year to developing technologies applicable to counterterrorism, mostly focusing on one large project. The United States Secret Service, another Treasury agency, has a clear interest in developing defenses against terrorism, but its research budget is quite modest (a few hundred thousand dollars per year). It depends on adapting the research of others to their needs.

Surprisingly, the Federal Bureau of Investigation, which has been given primary responsibility for responding to most domestic terrorist incidents, has a very small counterterrorism research budget. Its needs are closely aligned with those of the Department of Defense, and it makes liberal use of developments pioneered there.

A number of agencies have not been mentioned in detail in this report. Access to some (in the intelligence community) has not been obtained.

The Federal Research Effort Into Counterterrorism Technologies

For several reasons it is difficult to categorize unambiguously given activities of the various Federal agencies as directed specifically towards research into counterterrorism. For many agencies it is difficult to distinguish research performed for the main agency mission from that performed specifically for counterterrorism because the two efforts are often closely aligned. Also, some law enforcement activities, such as drug interdiction, frequently involve work that parallels counterterrorism research, but usually is distinct from it. Moreover, the line between research and development on the one hand and implementation on the other is not sharp; one frequently blends imperceptibly into the other as experience in the field is used to perfect an idea.

Table E-1 presents a partial list of agencies that have performed at least some research and development directly in, or at least applicable to, the field of counterterrorism.

The sections below discuss the activities of some of these organizations and, where the information is available, the main lines of research and funding levels.

Table E-l—Federal Agencies Engaged in Counterterrorism Research

Agency
Department of Defense
Department of Energy
EG&G (laboratories at Las Vegas and Santa Barbara)
Los Alamos National Laboratory (LANL)
Sandia National Laboratories (SNL)
Oak Ridge National Laboratory (ORNL)
Idaho National Engineering Laboratory (INEL)
Department of Justice
Federal Bureau of Investigation (FBI)
Immigration and Naturalization Service (INS)
National Institute of Justice
Department of State
Office of the Ambassador for Counterterrorism
Bureau of Diplomatic Security
Department of Transportation
Federal Aviation Administration (FAA)
Transportation Systems Center (TSC)
Department of the Treasury
Bureau of Alcohol, Tobacco, and firearms (BATF)
U.S. Customs Service (USCS)
U.S. Secret Service (USSS)
Environmental Protection Agency (EPA)
Interagency Intelligence Committee on Terrorism--Community Counterterrorism Board

SOURCE: Office of Technology Assessment, 1991.

National Counterterrorism Research and Development Program

Early in the 1970s, it was recognized that some sort of coordination would be necessary to establish clear lines of responsibility and maintain adequate channels of communication among these players. To this end, various groups and committees were established by every administration, beginning with President Nixon's. A consistent theme has been the lead agency concept, whereby a particular agency is given responsibility for responding to certain types of incidents. The following current lead agency assignments were developed during the Reagan Administration[1]:

- Department of State-incidents that take place outside U.S. territory,
- Department of Justice (FBI)--incidents that take place within U.S. territory, and
- Federal Aviation Administration (FAA)--incidents aboard aircraft in flight that take place within the special jurisdiction of the United States.

In addition, the tasks of coordination and communication still needed to be assigned. One organization charged with shouldering these duties is the Policy Coordinating Committee on Terrorism (PCC/T), originally known as the Interagency Group on Terrorism (IGT) when it was created in 1982. The committee has two important functions: 1) to bring cohesion to the overall U.S. Government counterterrorism effort and 2) to coordinate the programs of the member agencies for combating terrorism. chaired by the State Department's Coordinator for Counterterrorism, Ambassador Morris Busby, committee members are drawn from about 25 U.S. Government organizations. Within the committee, various working groups have been established, for example, the Public Diplomacy Working Group, which is designed to generate greater global understanding of the threat of terrorism and the efforts to resist it; and the Maritime Security Working Group, which assesses port and shipping vulnerabilities to terrorism.[2]

One of the most important subcommittees of the PCC/T is the Technical Support Working Group (TSWG), which administers the National Counterterrorism Research and Development Program. Through this program, research into promising technologies is supported by "seed money" grants. The idea is that, after prototyping, successful efforts will be picked up and implemented by one or another Federal, State, or local agency. The unique contribution of this group is that it is specifically designed to support research into technologies that would otherwise go undeveloped, either because other agencies do not find a sufficiently direct linkage to their mission or because they are concentrating their priorities on other projects.

The TSWG is cochaired by representatives of the Departments of Energy and Defense. Its members are drawn from an interagency group of scientists and technical and terrorism specialists organized into seven general areas: Threat Assessment and Database Management; Intrusion Detection and Countermeasures; Conventional Incident Response; Nuclear Incident Response; Chemical and Biological Incident Response; Explosives Disposal; and Technology Transfer. Some of the agencies participating in the TSWG include the Food and Drug Administration, the Environmental Protection Agency, the Federal Aviation Administration, the Federal Bureau of Investigation, the Department of Energy, the Department of the Army, the Department of the Navy, the Department of the Air Force and the Defense Intelligence Agency. Contacts with other nations have also been made.

A list of candidate technologies to be considered for inclusion in the program is developed periodically. After interagency discussion among the TSWG members, candidate projects are ranked based on priority and feasibility, and the ranked list is then submitted to the PCC/T Chairman for approval. Funds for the projects

[1] Public Report of the Vice President's Task Force on Combatting Terrorism, February 1986, P. 8.

[2] Ibid., p. 34.

come out of the budget of the State Department, but contracting and administrative support is provided at nominal expense (a few hundred thousand dollars per year) by the Department of Defense. One or more TSWG members supervise each project, with the research work actually being conducted either at the facilities of the member agencies or through subcontracting with various other laboratories and organizations both within and outside the Federal Government. Some of these are: Bendix Corp., Motorola Corp., the Illinois Institute of Technology, Los Alamos National Laboratory, the Naval Research Laboratory, and the Air Force Electronics System Division.

Funding for this effort was frost authorized by Congress in 1986 (Public Law 99-349). The appropriation is not a line item, but is-deeply embedded in the State Department's diplomatic security salaries and expenses account. The consequences of such fiscal anonymity are reflected in the consistently declining budget of the PCC/T. In its first year, 1986, riding a wave of public outrage over terrorist atrocities in the Middle East, the program was granted a budget of $10 million. These funds were part of a late supplemental appropriation and carried the program through fiscal year 1987. In fiscal year 1988, enthusiasm was beginning to wane. Of the $9 million requested, $7 million was appropriated. The next year, fiscal year 1989, as other priorities strained the national budget, the program became embroiled in battle over where, bureaucratically, such a research effort should be centered. Six million dollars were requested but only half that amount was approved, a compromise between the full funding appropriated by the House of Representatives and zero funding ordered by the Senate. Funding levels for fiscal year 1990 headed downward again, this time to the $2 million level. In fiscal year 1991, Congress agreed on an increase to $3 million, but internal funding reductions at the State Department made necessary by the budget agreement between Congress and the executive branch in late 1990 brought the actual number back to $2 million.

These cuts have resulted in termination or suspension of a number of projects because funding could not be assured. In an effort to keep the maxi-mum number of programs alive, a "good faith" or "matching funds" concept was implemented by TSWG, in which agencies participating in a research project were required to find funds to make up the difference between the amount allotted and the amount needed to run the project. Typically, the other agency had not planned on any expenditure of this nature and the last minute budget scramble was not always easy or successful. Such stop-and-go financing, while intended as a cost containment measure, is actually frequently counterproductive: it winds up killing some projects and adding to the ultimate price of others.[3]

Another handicap of a restricted budget is the absence of funds available even for the purpose of properly documenting the research that is conducted. Essentially all available dollars go into the research itself and there is little or no money left over to spend on disseminating the results. While a shoestring operation can sometimes produce useful work, more often than not the shoestring breaks before it can accomplish its mission.

The PCC/T staff asserts that an assured annual budget of at least $6 million would permit far more efficient operation.

PCC/T-TSWG Projects

In its short lifetime, the National Counterterrorism Research and Development Program has not had time or resources to complete many activities. Still, more than 50 projects have been proposed. Of these, almost 30 have been initiated and about 14 are at or near completion. A quick overview of several of these projects will show the breadth of the TSWG effort. Most items are reviewed in more detail in appendixes A through D.

The Transportable Emergency Response Monitoring Module

This project received $611,000 in fiscal year 1988 and $645,000 in fiscal year 1990. This unique, rapid response, transportable laboratory is designed for sustained operations in areas suspected of being contaminated by chemical or biological warfare agents. Instruments aboard the laboratory can detect, identify, quantify, and predict the spread of chemical and biological agents released by terrorists into water supplies and air. An interdisciplinary effort, the unit was designed and built by Engineering Computer Optecnomics, Inc. of Annapolis, MD using TSWG funds. The project manager came from the Environmental Protection Agency, and technical assistance was provided the U.S. Army's Chemical Research, Development, and Engineering Center (CRDEC). The unit will ultimately consist of two modules. Each unit will be about the size and shape of a semitrailer and is adapted for deployment by truck, helicopter, aircraft, railroad, ship, or barge. The analytical laboratory module, which has been constructed and can operate on its own, contains numerous pieces of modern laboratory equipment, all hardened to survive a not-too-gentle deployment. Air locks and decontamination showers are also provided. The living quarters module, construction of which has been delayed by lack of funds, will be attachable to the

[3]See, U.S. Congress, Office of Technology Assessment, "Introduction and Principal Findings," *The Defense Technology Base: Introduction and Overview—A Special Report,* OTA-ISC-374 (Washington, DC: U.S. Government Printing Office, March 1988), for a farther discussion of the problems associated with fluctuating research funding levels.

laboratory module and will provide completely self-contained operations for up to 7 days. This laboratory is uniquely capable of an on-the-spot response to a suspected chemical or biological attack. This effort has been successful despite a 1 year suspension in fiscal year 1989 due to lack of funds.

Expedient Hood

Also under the technical direction of CRDEC, this project resulted in the development of a prototype of an inexpensive, compact protective hood that could provide the wearer with 10 to 30 minutes of emergency ocular and respiratory protection against chemical or biological agents. The hood is now ready for further refinement by suitable agencies. The TSWG invested about $122,000 of its fiscal year 1989 funds in this project.

The Radiofrequency (RF) Quadruple Generator

The objective of this project was the development of a small, compact electronic neutron generating source for use in explosives detectors employed by airports. The unit was developed by ACCSYS Technology, located in Pleasanton, CA, and is designed to replace the radioactive neutron source currently used by explosives detectors based on thermal neutron analysis (see ch. 4 and app. A). A successful prototype has been produced. In fiscal year 1988 and fiscal year 1989 respectively, $248,000 and $125,000 of TSWG funds were allocated to this project.

Chemical Taggant for Plastic Explosives

In the spring of 1989, following the destruction of Pan Am Flight 103, two international groups held meetings to discuss what could be done to make small bombs carried aboard commercial aircraft easier to detect. Both groups determined that research should be conducted into suitable chemical taggants for the plastic explosives that constituted the main terrorist threat. Without the TSWG, there probably would not have been any U.S. contribution to this effort. On a minuscule budget of $35,000 supplied by the TSWG, a chemist from the Army's Armament Development Command at Picatinny Arsenal, NJ, was able to test the various proposed compounds and supply the United States representatives to these organizations with what would prove to be their only technical support.[4]

Remote Detection Instrument

The objective of this effort is to develop an early warning system capable of detecting and identifying chemical agents at least 1 kilometer away using an infrared laser. In fiscal year 1988, this project received $428,000 from the TSWG and $405,000 in fiscal year 1990. The U.S. Army Chemical Research, Development and Engineering Center in Maryland is working with the SRI Corp. of California in the development of this instrument.

This incomplete list gives at least a flavor for the depth and breadth of efforts that the TSWG has supported or sponsored.

Other Agencies

This section contains descriptions of some of the work performed by other agencies, including efforts to deter or prevent terrorist acts as well as preparations for coping with a terrorist incident once it develops.

Department of Defense

Agencies Within Department of Defense

Relevant budget: fiscal year 1990-about $11 million

Several agencies are working on terrorism-related projects, covering fields such as explosives detection, threat prediction, and physical security. The latter field represents a major part of this group of efforts.

DoD has a budget of about $40 million per year devoted to physical security. Of this, about $5 million is allocated for exploratory development. Most of these projects involve development of novel means to detect and/or disable intruders. For example, one project includes a van or truck equipped with a combination of two infrared detectors capable of finding and tracking an intruder at a significant distance. Other detection strategies involve the use of various combinations of seismic, acoustic, infrared, and electrical sensors. Less esoteric undertakings are directed at improving physical barriers such as fences. Some agencies within DoD have been cooperating on joint ventures with other DoD agencies and with each other. For example, one agency has worked with the Department of State on strategies for hardening our embassies and other facilities overseas and two DoD agencies have worked on the development of an early warning threat detection system, having shared startup funds for this project.

Several programs under the aegis of these agencies within DoD have been transferred to the U.S. Navy. These include the acoustic lens sonar and the multifunctional sensor programs. Other Navy-specific programs include a Swimmer Identification System, which will provide an autonomous alarm system for detection of surface and subsurface swimmers; Waterside Lightweight Barriers, which will provide protection against high-speed, explosive laden boats; an Underwater Security Vehicle for positive identification of underwater intruders, and several other programs designed to meet the Navy's opera-

[4]However, from fiscal year 1989 through fiscal year 1991, a cumulative total of $285,000 was provided by TSWG to the Armament Development Commaud for a tagging plastic explosives project.

tional requirements for Waterside and Shipboard Security Systems.

Military Services

Relevant budget: for fiscal year 1990,$16 million directly for counterterrorist activities

For fiscal year 1990, the Army allocated about $167 million to research activities that might be characterized as pertaining to the fight against terrorism. For fiscal year 1991, the Army expects to invest about an equivalent amount. This research includes literally dozens of projects aimed at developing materiel, munitions, equipment, and procedures for supporting special operations and dealing with low-intensity conflict. Many of these efforts are suitable in a counterterrorist context as well, although few are specifically designated as such.

The following groups contribute to Army R&D applicable to counterterrorism, roughly ranked by size of their effort:

- Chemical Research, Development, and Engineering Center;
- U.S. Army Medical Research Institute of Infectious Diseases;
- U.S. Army Medical Research Institute of Chemical Defense;
- Aviation Systems Command;
- Natick Research, Development, and Engineering Center;
- Communications-Electronics Command;
- Belvoir Research, Development, and Engineering Center;
- Army Research Office;
- Corps of Engineers; and
- Atmospheric Sciences Laboratory.

The Army is a member of the PCC/T (described above) and its Technical Support Working Group particularly in the areas of Threat Assessment, Intrusion Detection Countermeasures, and Chem/Bio Incident Response R&D. It also is involved with other interagency efforts.

The main line of investigation (about 85 percent of the research budget) is directed at defense against chemical or biological weapons, reflecting the Army's role as the DoD executive agent for chemical and biological defense research. This work can be broken down into four categories:

1. reconnaissance, detection, and identification;
2. protection;
3. decontamination; and
4. medical diagnosis and casualty care.

For example, at the Army Atmospheric Sciences Laboratory, research is being done into using computer modeling to predict the spread and dispersion of an aerosol agent. Also, work is being done to develop light weight overgarments that troops could wear to protect against toxic or biological threats. Further, a system for remotely monitoring the vital signs of a soldier is being developed. This would allow quick medical decisions to be made, even in a contaminated environment. Other lines of research include intrusion detection, physical security, explosives detection, and incident response.

While most of this activity is related to counterterrorism only as an off-shoot of the direct research mission, at least one Army program is specifically targeted towards research into counterterrorism technologies. Within the Chemical Research, Development, and Engineering Center lies the Chemical/Biological Antiterrorism program. This small unit (fiscal year 1989 budget = $99,000 of Army funds, $6.2 million customer (that is to say, non-Army) funds), is charged with development of protective gear, decontamination equipment, detection/identification equipment and less-than-lethal techniques specifically to cope with terrorist incidents. This group also provides technical support for other government agencies in the field of countering the threat of chemical/biological terrorism. In particular, the TSWG, the U.S. Secret Service, the National Institute of Justice, the Federal Bureau of Investigation, and other DoD agencies make use of the counter/antiterrorism[5] expertise of this group.

In addition, the Army has allocated some $10 million in fiscal year 1990 for R&D specifically aimed at developing technology for combatting terrorism in special operations contexts. Other services together have allocated an additional $6 million to this end.

Department of Energy

Relevant budget: $6 million for fiscal year 1989

Through its Special Technologies Program, the Department of Energy (DoE) is doing a considerable amount of work in areas useful to the fight against terrorism. Much of this effort, handled at DoE's Laboratories in Las Vegas and Santa Barbara, CA, is related to DoE's responsibilities under the Atomic Energy Act. A large, separate but related, budget is devoted to development and support of the Nuclear Emergency Support Teams (NEST), whose mission is to find and recover purloined nuclear material and provide technical support to other government agencies in responding to radiological threats. Additional funds are spent by the safeguards and security program, primarily in antiterrorism. There is a substantial amount of work in the area of remote detection of nuclear material

[5] ''Antiterrorism'' is the term used by the military to refer to passive defenses against terrorism. "Countertermrism" refers to active responses to terrorist attacks. This report employs the latter term for both purposes, since it is generally understood as such by the public.

and nuclear weapons. In addition, a significant effort exists, in collaboration with the Naval Explosive Ordnance Disposal Technology Center, in developing means of detecting and countering alarm systems, especially those based on infrared or microwave, and acoustic technologies. However, several laboratories are involved in development of other counterterrorist techniques, many funded not out of the $6 million referred to above, but out of laboratory funds for other programs, or out of reimbursable contracts from other Federal agencies.

Los Alamos National Laboratory (LANL)

A substantial amount of work related to counterterrorism is performed at LANL. One area of work is in diagnostics and disablement, which includes research aimed at bolstering defenses against nuclear terrorism. Another set of efforts is in a program of R&D in low intensity conflict, special operations, counterterrorism, and counternarcotics. This program spent about $19 million in fiscal year 1989, of which perhaps $9 million was devoted to counterterrorism. Most of the funding is in reimbursable projects from other government agencies and some is from the TSWG. Some typical fields of research include methods of early detection of chemical and biological agents, miniaturized radar for remote emplacement, and development of computer techniques for analyzing large quantities of real-time financial data to detect money laundering. Other divisions of LANL are involved in advanced technologies for explosives detection and laser means for remote detection of biological agents.

Sandia National Laboratories (SNL)

SNL is the lead laboratory within DoE for R&D into physical security, and as such is active in the development and evaluation of numerous devices applicable to counterterrorism. In particular, it conducts tests and evaluations of explosives detectors, intrusion detectors, and metal detectors. It has explored various schemes for access control, especially rapid identity verification, including voice print, hand profile, retina scan, finger prints, and signature dynamics. Research has also been carried out on barriers to intrusion such as smoke and foams.

In addition, for many years, SNL has had a program of evaluation and development in both explosives detection and weapons detection. There has been a significant transfer of experience and technology to the private sector in these areas.

Sandia Laboratories is being funded by the FAA's Technical Center to develop a systems approach to airport security, the "Enhanced Security Demonstration Project' for BWI airport near Baltimore, MD, discussed in chapter 4. Low intensity conflict has been another area of research for Sandia that is of interest to counterterrorism. In this field, it is investigating remote sensors, portable satellite communication, and alarm and annunciator systems for noncombatants in a danger area.

Sandia has also been working with the FBI, Customs and the INS especially in the field of counter narcotics, having been designated a ''center of excellence" for this purpose under Public Law 100-790. This work especially involves development of such items as night vision equipment and motion sensors.

Oak Ridge National Laboratory

About $400,000 per year for the last 3 years has been invested by DoE at its Oak Ridge National Laboratory in Oak Ridge, TN for the development of a mass spectrometer capable of detecting and identifying tiny amounts of vapor emitted by plastic explosives. Additional fiscal year 1990 funds have been utilized to seed technologies that have counterterrorism applications.

Idaho National Engineering Laboratory

About $400,000 per year has also been invested by DoE at its Idaho National Engineering Laboratory (INEL). Additional fiscal year 1990 funds have also been utilized here to seed technologies which have counterterrorism applications.

Department of Justice

Federal Bureau of Investigation

Relevant budget: small-exact figure not available at this time

The FBI's Hostage Rescue Team has responsibility for events, including terrorist incidents, that involve Federal or interstate jurisdiction. They do very little R&D, being mostly an operational unit. However, they have channeled some DoD funds (approximately $1 to $2 million per year) to outside contractors for relevant research.

The Special Operations Research Unit is working on less-than-lethal weapons and incapacitating agents; some of this work is sponsored by the National Institute of Justice. The Forensic Science Center performs work on evaluation of explosives detectors. In particular, in March of 1988, the Center performed a meticulous series of "real-world' tests on a group of explosives vapors detectors representative of then commercially available models.[6] The total research budget of this center is $300,000 for fiscal year 1990, half of that available in earlier years. Only part of this budget is devoted specifically to counterterrorist activity. The FBI also

[6] See *Explosives Detector Evaluation*, a limited distribution report produced by the FBI Laboratory, Forensic Science Research an Training Center, FBI Academy, Quantico, VA 22135, Mar. 21-24, 1988. Registered copies for official use are available by writing to the above address on letterhead.

supports the explosives detection community in two other ways. Every October, they sponsor and organize a symposium to discuss current R&D efforts. Also, the FBI Laboratory analyzes all samples of foreign explosives gathered by other law enforcement agencies.

Immigration and Naturalization Service (INS)

Relevant budget: $400,000 for fiscal year 1990

This service has ongoing R&D efforts in the area of facial recognition and technologies related to document verification. The Service's Forensic Laboratory has no funds available for research and development.

National Institute of Justice

Relevant budget: $500,000 for fiscal year 1989 (to CRDEC)

This money funded work on less-than-lethal agents. Similar work was channeled through the FBI to other contractors.

Department of State

Office of the Ambassador for Counterterrorism (Technical Support Working Group)

Relevant budget: fiscal year 1986-87--$10 million
fiscal year 1988--$7 million
fiscal year 1989--$3 million
fiscal year 1990--$2 million

See chapters 1 and 4 and above sections in this appendix for more information on this project.

Bureau of Diplomatic Security

Relevant budget: fiscal years 1986-9=6.5 million for explosives detection; the current budget includes $300,000 to $400,000 per year on other research.

This office is responsible for assuring the security of State Department property and personnel. The largest part of its research budget has been expended in supporting the development of an explosives "sniffer." See appendix C of this report for information on the Thermedics, Inc. explosive detector. A much smaller budget is devoted to research into alarms, locks, closed-circuit TV, blast hardening of buildings, and technical countermeasures to mask radio signals. Finally, some work is being conducted in cooperation with the intelligence community.

Department of Transportation

Federal Aviation Administration

Relevant budget: see table E-2

The FAA Technical Center, located in Atlantic City, NJ, manages a wide range of research programs aimed at developing systems and devices to prevent aviation related hijacking and sabotage. These include efforts aimed at explosives detection, airport security, and security systems integration. Perhaps its best known field of investigation is the thermal neutron analysis (TNA) technique of explosives detection, discussed in detail in chapter 4 and appendix A. It has also heavily funded the development of the chemiluminescent-based explosives vapor detection equipment especially as a portal monitor for concourse security. Other technical approaches to explosives detection currently under investigation are:

- *vapor approaches* (which seek to detect molecules of explosives in the air or on external surfaces):
  —Advanced Ion Mobility
  -Surface Acoustic Wave
  —Modulated Infrared Absorption
  —Preconcentration
- *bulk approaches* (which use various types of penetrating radiation to interact with an explosive hidden inside a package, producing detectable secondary radiation):
  —Nuclear Resonance Absorption
  —Fast Neutron Scattering
  —Nuclear Magnetic Resonance
  —Expert Systems (not a detection technique in itself, but the use of computer software in support of bulk approaches)

The agency is working to expand this list. In an effort to attract numerous new strategies and approaches for explosives detection, the FAA has recently issued a Broad Agency Announcement. They are also sponsoring or attending numerous seminars and interagency and international symposia to improve research efforts in this area.

A large part of the FAA's research budget for the next several years ($3 million for fiscal year 1990) will be devoted to the BWI Airport Demonstration project. This project has enlisted the technical expertise of DoE's Sandia National Laboratories to assist in the development of a complete systems approach to airport security including access control as well as explosives and weapons detection.

Funding for major programs for fiscal year 1990 are listed in table E-3.

Department of the Treasury

Bureau of Alcohol, Tobacco, and Firearms

This agency has some research activity of indirect relevance to counterterrorism. In the area of communications, it is participating in an interagency law enforcement effort to standardize communications for multiagency operations. This is mainly aimed at drug enforcement and is being coordinated by the Office of National Drug Control Policy. The agency is also looking at ways of tracking items (i.e., people, vehicles, contraband) by

Table E-2—Allocation of FAA Security R&D Resources

	Resources ($ thousands)					
	Fiscal year 1990			Fiscal year 1991 (requested)		
	Contract	Manpower	Total	Contract	Manpower	Total
Explosives detection	7,000	850	7,850	22,018	597	22,615
Weapons detection	1,500	300	1,800	1,500	399	1,899
Airport and system integration	3,513	207	3,720	1,500	348	1,848
Total	12,013	1,357	13,370	25,018	1,344	26,362

SOURCE: Federal Aviation Administration, 1990.

Table E-3-Allocation of FAA Fiscal Year 1990 Contract Dollars for Major Program Priorities

Major program priorities	Contract allocations ($ millions)
Thermal Neutron/Dual Sensor Support	$0.5
Vapor Portal Development	1.8
New Technology Explosives Detection	4.5
New Technology Weapons Detection	1.2
Commercial Security Systems Evaluation	0.5
BWI Airport Demonstration	3.0
Other, efforts	0.5
Total	$12.0

SOURCE: Federal Aviation Administration, 1990.

means of satellite systems. Other efforts more closely related to counterterrorism are the International Explosives Incident System, a repository for data related to international incidents involving explosives; and the international taggant study conducted under the auspices of the International Civil Aviation Organization (see ch. 4).

U.S. Customs Service

Relevant budget: approximately $4.8 million per year for last 3 years.

This agency does not engage in much original research directly related to counter terrorism. However, Customs has supported considerable work in the area of drug detection and interdiction, some of which is of ancillary utility to the war on terrorism. The largest portion of the R&D money mentioned above (about $3 million per year) has been devoted to development of a covert remote locating system (known as Geostar). Signals from a small device hidden on an object will be picked up by a pair of Earth satellites. By triangulation, the location of the object can be determined. This project is a cooperative effort with other agencies and groups, including the TSWG.

The remaining funds go primarily into contraband and drug detection equipment. As an example, Customs is sponsoring the development of an automatic letter mail examiner for the detection of heroin, cocaine, and morphine by the use of Nuclear Magnetic Resonance. Laboratory and advanced prototyping efforts have shown this technology also to be amenable to explosives detection. In a current joint Customs-FAA project, single-sided imaging using gamma ray backscatter technology is being developed for contraband (including explosives) detection. The system is close to acceptance. Customs also funded and designed a mobile x-ray capability suitable for planeside examination of baggage and cargo. This agency also relies on other agencies, DoD or CIA for example, which share some specific R&D goals.

An interesting project being undertaken by Customs is an improvement of their Advanced Passenger Information System (APIS), which is an automated system for screening passengers. In cooperation with a number of agencies interested in monitoring travelers (INS and DEA for example), a large database is being assembled that contains information on known undesirables. Through a computer workstation, an inspector can access this database using a name, passport, or visa number. An enhancement that is being explored would make possible a computer comparison of a traveler's appearance with a stored image of suspects.

U.S. Secret Service

Relevant budget: fiscal year 1990-a few hundred thousand dollars

Secret Service participates in the TSWG and does not have a large research budget, since it is more of a user than developer. It has participated in several TSWG projects. Further, it has, on its own, worked on perfecting a software package that can estimate the effects of bombs on a building of given size and construction. Specifically, this package is designed to improve security by identifying the most vulnerable areas of a building or to provide forensic information on the probable size and location of an explosive from post-blast data. The output of the computer program will aid in planning inspections of structures before the arrival of key officials. Secret Service officials are anxious to maintain funding for this project. If the risk from bomb blast could be accurately defined, they argue, searches and guard postings could be much more efficiently executed thereby saving time, effort, and money.

Environmental Protection Agency (EPA)

The EPA is managing the TSWG-funded project to develop the mobile laboratory to respond to chemical and biological terrorist attacks, described above in this appendix.

Interagency Intelligence Committee on Terrorism—Community Counterterrorism Board

This group is made up of representatives from various agencies involved with intelligence issues. It includes a Research and Development subcommittee that oversees research that would aid in data analysis as well as other areas of special interest to the intelligence community.

Appendix F

Congressional Request and Support Letters

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

June 22, 1989

The Honorable John H. Gibbons
Director, Office of Technology Assessment
United States Congress
Washington, D. C. 20510-8025

Dear Dr. Gibbons:

We are writing to request that OTA conduct a study to identify and assess those technologies that could provide the Nation with tools in the fight against terrorism.

The past two decades have seen a steep rise in terrorist actions, often directed at U.S. targets, including civilians. Attacks have included kidnappings, hijackings and bombings of civilian aircraft, as well as bombings of U.S. economic or military targets. The case of Pan Am 103 is only the most recent and most striking of a long series of such incidents. Moreover, statements by Iranian leaders lead us to expect that terrorist attacks against American citizens throughout the world may increase.

The practical difficulty of responding to terrorist attacks has been apparent. Since terror consists of limited actions often directed at civilians, military tactics and technologies are frequently not applicable, either in preventing an occurrence or in dealing with an ongoing one.

For example, highly intrusive and costly security measures, which the military or police agencies can employ, could make the successful emplacement of explosive devices on civilian aircraft very difficult. But they might also paralyze air travel and commerce, as well as intrude on many Americans' concept of a free society. As another example, if passengers were taken hostage aboard an aircraft, a classic military assault to retake the aircraft would seriously endanger the hostages.

One strong asset that the U.S. possesses is its high level of technological development. We would like to assure ourselves that the Nation is taking full advantage of its capabilities in this area. While we are aware that there is no

The Honorable John H. Gibbons
June 22, 1989
Page Two

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 required, military or para-military action.

Therefore, we would like OTA to review the current status of research, federally-funded and other, aimed at developing counter-terrorist tools. The review should also assess research and development that, while not explicitly developed for counter-terrorism, might have applications in that area. It should include, but not necessarily be limited to explosives detectors, methods of access and perimeter control, non-lethal but disabling weapons, incapacitating agents, and improved data exchange on terrorism and terrorist techniques. In carrying out this study, classified research and development activities within federal agencies should be examined, along with open sources.

The report should assess whether federally-funded research in this area is well coordinated and sufficiently focused. It should also identify those areas where increased resources would be helpful in producing positive results in the short-term. We do not expect the study to deal with intelligence gathering or with police or military tactics.

We anticipate that the final report will be unclassified. However, in order to avoid putting useful material into the hands of potential terrorists, we expect that OTA will also produce a substantial classified annex that would accompany the report. An interim report should be provided to the Committee by March 1, 1990. The final report should be furnished no later than December 31, 1990.

Sincerely,

John Glenn
Chairman

William V. Roth, Jr.
Ranking Minority Member

JHG/mkh

United States Senate
COMMITTEE ON FOREIGN RELATIONS
WASHINGTON, DC 20510-6225

July *6, 1989*

Dr. John H. Gibbons
Office of Technology Assessment
600 Pennsylvania Avenue
Washington DC 20510

Dear Dr. Gibbons:

As the tragic downing of Pan Am 103 demonstrated last year, terrorism continues to exact its toll on Americans. Combatting terrorism remains a difficult task for all governments, and the United States and its citizens remain a significant target of a number of terrorism organizations.

As Chairman and Ranking Member of the Senate Foreign Relations Committee Subcommittee on Terrorism, Narcotics and International Operations, we are writing to request that OTA conduct a study to identify and assess technologies that can provide the U.S. with tools in the fight against terrorism.

In recent years, we have seen a steep rise in terrorist actions, including kidnappings, hijackings and bombings of civilian aircraft, as well as bombings of U.S. economic or military targets. Statements by Iranian leaders, and reports of continued terrorist activity by a variety of foreign political and military organizations, lead us to expect that terrorist attacks against American citizens throughout the world may increase.

The Pan Am attack highlighted the difficulties of responding to intelligence about possible terrorist attacks, as well some of the limitations of current anti-terorrist detection equipment.

To date, we know of no study available to the Congress which has undertaken a comprehensive review of anti-terrorist technologies, with a view of assisting the Congress in determining how we can better fight terrorism.

Accordingly, we request that OTA conduct a study of current and possible future U.S. anti-terrorism technologies.

2

The review would assess those technologies now in place; review the current status of research, federally-funded and other, aimed at -developing counter-terrorist tools; and assess research and development that, while not explicitly developed for counter-terrorism, might have applications in that area.

We would appreciate the study also including a review of the capabilities of specific technologies such as explosives detectors and incapacitating agents. We believe it would also be helpful for the Congress to understand the current limits and capabilities of data collection and exchanges on terrorism, (in terms of the technologies used to move information from one network to another), as well as the techniques used by terrorists in committing terrorist acts.

The report should assess whether federally-funded research in this area is well coordinated and sufficiently focused, and to identify those areas where increased resources would be helpful in producing positive results in the short-term. To carry this study out properly, we believe OTA should rely on both classified research and development activities within federal agencies and open sources.

We anticipate that the final report will be unclassified. However, in order to avoid putting useful material into the hands of potential terrorists, we expect that OTA will also produce a substantial classified annex that would accompany the report. An interim report should be provided to the committee by March 1, 1990. The final report should be furnished no later than December 31, 1990.

We very much appreciate your attention to this request.

Sincerely,

Mitch McConnell
Ranking Member

John Kerry
Chairman

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

August 3, 1989

The Honorable John H. Gibbons
Director, Off ice of Technology Assessment
United States Congress
Washington, D. C. 20510-8025

Dear Dr. Gibbons:

The bombing of Pan Am Flight 103 last December is only the most recent in a series of attacks on American civilian aircraft by terrorists. Given our jurisdiction over aviation security, we are concerned about protecting the safety of American travelers at home and abroad, particularly with respect to utilizing the most effective advanced technologies for airport security screening.

Although we are aware that there is no certain technical fix for terrorism, we would like to assure that the Nation is taking full advantage of its technological capabilities. Accordingly, we request OTA to review the current status of Federally-funded and other research aimed at developing tools for providing airport security.

The study should assess research and development on explosive detection devices, including those capable of detecting very small amounts of explosives; methods of access control; human factors; and improved data exchange. Classified research and development activities within the Federal agencies as well as other sources should be examined. The study should also address the degree to which Federally-funded research in this area is coordinated and focused, as well as those areas where increased resources might help to bring positive results in the short-term.

- 2 -

We anticipate that the final report will be unclassified, with the option of a classified appendix. It would be helpful to the Committee to have an interim report in the spring of 1990, with the final report submitted by the end of 1990.

Sincerely,

ERNEST F. HOLLINGS
Chairman

WENDELL H. FORD
Chairman
Aviation Subcommittee

JOHN C. DANFORTH
Ranking Minority

JOHN MCCAIN
Ranking Minority

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 10510-6475

June 7, 1990

SSCI #90-2534

Dr. John H. Gibbons
Director
Congress of the United States
Office of Technology Assessment
Washington, D.C. 20510-8025

Dear Dr. Gibbons:

We understand that the Office of Technology Assessment is currently engaged in a study of the uses of technology to combat terrorism. This study is being "conducted at the request of the Senate Governmental Affairs Committee, the Senate Commerce Committee s Subcommittee on Aviation, and the Subcommittee on Terrorism, Narcotics and International Operations of the Senate Foreign Relations Committee. It is our understanding that the study will include an-examination of federal research and development efforts in this area. The Senate Select Committee on Intelligence endorses the requests of these committees and strongly supports this work, which, we hope, will provide useful information in assessing the effectiveness and the degree of interagency coordination of such activities.

Accordingly, the Senate Intelligence Committee wishes to be kept fully informed of the progress of OTA'S work on this project and to receive related publications and briefings as soon as they are available. The point of contact on our staff is Charles Battaglia at 4-1765.

Sincerely,

David L. Boren
Chairman

William S. Cohen
Vice Chairman