Technology Against Terrorism: Structuring Security

January 1992

OTA-ISC-511
NTIS order #PB92-152529

TECHNOLOGY AGAINST TERRORISM

STRUCTURING SECURITY

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Technology Against Terrorism: Structuring Security, OTA-ISC-511* (Washington, DC: U.S. Government Printing Office, January 1992).

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop SS0p. Washington, D.C. 20402-9328
ISBN 0-16 -036061-7

Foreword

Terrorism is not a new phenomenon, but it has become more prominent during the past two decades. Terrorist attacks have included not only political assassinations, but also large-scale attacks, often aimed at third parties, causing massive casualties. Two well-known examples are car bombings, employing hundreds of kilograms of high explosives, and attacks on commercial aircraft around the world. The U.S. Government and the American public became acutely aware of terrorism after the bombing of Pan American Flight 103 over Lockerbie, Scotland in December 1988. The recent war in the Persian Gulf heightened fears of renewed terrorist attacks on U.S. targets, both overseas and at home.

In 1989, because of growing concern over terrorist threats, several Senate Committees requested that OTA study the role of technology in fighting terrorism and the Federal effort in promoting related research and development. The requesting Committees were: Governmental Affairs; Foreign Relations (Subcommittee on Terrorism, Narcotics, and International Operations); and Commerce, Science, and Transportation, together with its Subcommittee on Aviation. The Senate Select Committee on Intelligence also endorsed the study.

This report is the second and final one in response to these requests. The frost was transmitted to Congress in a classified version in September 1990. An unclassified summary was released to the public separately in February 1991, and an unclassified version of the full report was published in July 1991. This second report also has a classified annex with additional technical data. The first report concentrated on Federal funding for research and development in counterterrorist technology and on aspects of airline security, particularly explosives detection. This report is devoted primarily to three other topics: interagency coordination of efforts in counterterrorist research and development, integrated security systems, and the role of human factors in aviation security. In addition, it furnishes details on a number of technologies that play a role in counterterrorism.

The help and cooperation of a large number of scientists and officials from the Departments of Defense, Justice, State, Transportation, and the Treasury are gratefully acknowledged. Special thanks are due to the Federal Aviation Administration.

JOHN H. GIBBONS
Director

The Use of Technology in Countering Terrorism
Advisory Panel

Marvin Goldberger, *Chairman*
Director, Institute of Advanced Study

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

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

Homer Boynton
Managing Director for Security
American Airlines

L. Paul Bremer
Managing Director
Kissinger Associates, Inc.

Chris Chicles
Security Managing Consultant
C.H. Chicles & Associates

Arthur Donahue
President of Marketing
Softworld, Inc.

Lee Grodzins
Department of Physics
Massachusetts Institute of Technology

John (Chris) Hatcher
Department of Psychiatry
Center for the Study of Trauma
University of CA, San Francisco

Carolyn Imamura
Director of Planning and Programs
Pacific Basin Development Council

Wilfred Jackson
Airport Operators Council, Intl.

James Jacobs
Director, Nuclear Security Systems
Sandia National Laboratory

Brian Jenkins
Managing Director
Kroll Associates

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

Donald Kerr
President
EG&G, Inc.

Joseph Krofcheck
President
Yarrow Associates

Robert Kupperman
Senior Adviser
Center for Strategic and International Studies

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

Richard Porter
Aerospace Services International, Inc.

Billie H. Vincent
Aerospace Services International, Inc.

Stanley Wiener
Professor of Internal Medicine
University of Illinois, Chicago

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 Callaham

Kevin Dopart[1]

Deborah L. Kyle[2]

Russell L. Maxwe11[3]

Edith Page[4]

Peter H. Rose[5]

Administrative Staff

Jacqueline R. Boykin

Louise Staley

Contractor

Yonah Alexander

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

Contents

Chapter 1

Summary

Contents

Chapter 1
Summary

INTRODUCTION

In 1991, the Persian Gulf War drew the world's attention once again to the threat of terrorism.[1] Fears arose that Iraqi agents, their surrogates, and their allies would use the terrorist option as other options became foreclosed to them. These concerns stimulated unprecedented security measures across the world, at government and public buildings both in Washington and in the capitals of other coalition states, at diplomatic sites, and at international airports on all continents. In the end, no major incidents occurred (although a number of minor ones did take place), perhaps because of the intensive security measures taken. In many countries, suspected Iraqi agents were either deported or detained, which may have had a telling effect on efforts to organize successful major attacks. Nevertheless, in the first few weeks following the outbreak of hostilities in January 1991, the number of international terrorist incidents against U.S. targets did increase significantly over the same period in the previous year. Only one, however, was directly traceable to Iraq: a failed attempt to blow up the U.S. Information Agency building in Manila. Another, possibly linked directly to the Gulf War, was an attempt to explode a bomb at the residence of the U.S. Ambassador to Indonesia in Jakarta. In general, the increase in terrorist incidents appeared to be the result of uncoordinated actions of solidarity with the Iraqi regime on the part of anti-U.S. elements in a number of countries.

Although no major terrorist actions in connection with the Gulf War have yet occurred, such eventualities cannot be excluded in the near future. There have often been lapses of months or years between an event and a terrorist response. Such actions are often complicated operations that require a lot of time to plan and execute.

Even apart from tensions in the Gulf and the Middle East, terrorism has not been quiescent since the start of this study in September 1989. The most startling recent single event was the assassination of Rajiv Gandhi in the midst of Indian parliamentary elections in May 1991. Other examples of continuing terrorism include the massacres of scores of rail passengers in separate incidents by terrorists in India and in South Africa. In Europe, terrorists have been active, particularly in Spain, Northern Ireland, and Germany. Single-issue terrorists (e.g., antiabortion zealots, animal rights extremists) are still active in the United States and Western Europe. Other domestic terrorism in the United States, while currently at a low level, may resurge periodically. The phenomenon is global in scope and, unfortunately, continues to demand attention and protective action by the civilized world.

As terrorist tactics change, it will become increasingly important to be proactive rather than reactive in developing technologies to protect the public. Future threats should be anticipated to the degree possible so that means for dealing with them will be developed in a timely manner.

This report concludes an examination of the role that technology may play in the effort to combat terrorism. It is the second of two reports, which together constitute an assessment of the role of technology in combating terrorism. Requested by three Senate committees in the summer of 1989,[2] and begun in September 1989, the first report of the study, *Technology Against Terrorism: The Federal*

---

[1] This assessment uses a working definition of terrorism, presented in the first OTA report in this series, U.S. congress, office of Technology Assessment, *TechnologyAgainst Terrrorism: The Federal Effort,* OTA-ISC-481 (Washington, DC: U.S. Government Printing Office, July 1991), pp. 16-17:

> **The deliberate employment of violence or the threat of use 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 create a climate of fear in a target population larger than the civilian or military victims attacked or threatened.**

This definotion covers a wide variety of violent acts against non-combatants, ranging from attacks on clinics by foes of abortion to mass murder by sophisticated international terrorist groups (e.g., attacks on commercial aviation).

[2] The requesting committees are the Committee on Governmental Affairs, the Subcommittee on Terrorism, Narcotics and International Operations of the Committee on Foreign Relations, and the Committee on Commerce, Science, and Transportation and its Aviation Subcommittee. In addition, the Senate Select Committee on Intelligence later endorsed the study.

Effort,[3] *was* delivered to the committees in September 1990. It summarized the research programs developed by many government agencies for countering terrorist activities and investigated the state of the art of some airline security technologies, notably explosives detectors. Several findings were reached that involved first, the overall Federal funding of such research and development (R&D), the interagency component of that effort, and the program to develop explosives detectors, especially for airline security.

This report covers a number of remaining areas and provides updated information on research progress in a number of fields. It discusses four principal topics that were not previously dealt with in detail: the terrorist threat from biological agents; interagency and international cooperation in R&D aimed at counterterrorism; the application of an integrated systems approach for aviation security; and the role of human factors in security.

In addition to the findings and supporting information and analysis, this study contains a compendium of technical information on counterterrorist R&D and technology to add to that of the past report. Together, the two volumes include a survey of most of the relevant work going on in the general field, and should provide a useful reference on the state of the technology at the time of publication.

OUTLINE OF REPORT

This chapter presents a summary and findings of the report. The second chapter discusses a revised update of the terrorist threat, as of June 1991. First, some recent examples of terrorist attacks are given to provide a sketch of the latest trends in targets, tactics, techniques, and technologies used. The implications of the Gulf War on potential future threats are also presented. Further, the chapter provides some insights on current players and organizations on the terrorist scene. Finally, a detailed discussion of the nature of potential biological terrorist threats is presented.

The third chapter presents the problems that arise when many different agencies (and countries) work in parallel on the counterterrorism problem. There are difficulties with sharing information, with coordinating responses, and with coordinating R&D. Some past problems are being successfully addressed, while others need more attention. The report presents several options that Congress may wish to consider to deal with the issue of improving interagency coordination.

The fourth chapter discusses strategies for designing integrated systems for airline security. In particular, it makes some suggestions for approaches that combine different types of explosives detectors in a system that would be more effective and less expensive than relying on just one type of device.

Chapter 5 discusses the application of the study of human factors to airline security, a heretofore neglected field that is now drawing deserved attention. The best equipment available will not provide adequate security, even when automated to a high degree and when successfully integrating many different techniques, unless the humans running it are able to operate it well. Humans must be able to analyze properly the information that is provided by the mechanical and electronic parts of the system, and to use those elements to respond in timely and correct fashion to alarms or attacks.

The next two chapters are presented in SECRET versions only. Chapter 6 discusses technologies available and under development, for assisting law enforcement authorities and the military in responding to terrorist incidents. Chapter 7 presents a survey of the emerging field of less-than-lethal weapons. The desirability of disabling, while not permanently harming, individuals within weapon range is clear in the case of terrorists holding hostages. In addition, such techniques, if successfully developed, could revolutionize warfare, especially in the area of low-intensity conflict.

The final part of the report consists of a set of appendixes that gives technical background on several topics. This information complements material found in this and the earlier report. Appendix A discusses the Federal Aviation Administration's (FAA) R&D program for airline security. Following recent criticism from a number of sources (including OTA), the FAA has taken major steps to reorient and refocus its program. The changes and new directions of research are outlined here.

Appendix B discusses the role of animals, notably dogs, in explosives detection. In many contexts, carefully selected and trained dogs remain the

[3]U.S. Congress, Office of Technology Assessment, op. cit., footnote 1.

detector of choice, although their abilities may often complement technical means of accomplishing the same ends.

Appendix C presents the state of the art in metal and weapons detectors.

In appendix D, technologies are presented that are applicable to defending harbors and ports against terrorist attacks. Of special interest is the protection of tourist ships, which have already been targeted on a number of occasions by Middle Eastern terrorist groups.

Appendix E contains a summary of equipment, generally available and in wide use, used for placing barriers, sensors, and alarms around fixed sites and for controlling access to them. It also contains some discussion of technologies to incorporate into building design for defending against terrorist bombings. The techniques covered in this chapter are applicable to many types of sites, from military and nuclear installations (where such systems are installed and have been for a long time) to U.S. Government buildings that might be considered tempting terrorist targets, such as embassies and consulates, to buildings belonging to private corporations.

The last three appendixes are only available in classified versions. Appendix F (CONFIDENTIAL) reviews the work being done in the area of electromagnetic techniques of detecting explosives, particularly nuclear magnetic and nuclear quadruple resonance. Appendix G (SECRET) describes possible responses to the threat of surface-to-air missiles. Finally, Appendix H (SECRET) gives a summary of information on effects of biological agents and on the capabilities of some states in this area. The classified portions of the report are available from OTA to those with the proper clearances and a need to know.

FINDINGS

Chemical and Biological Terrorism

FINDING 1

Interagency coordination for responding to chemical and biological (CB) terrorism has shown marked (and sorely needed) improvement recently. An interagency plan to respond to such eventualities now exists. However, more coordination and more R&D are needed to improve response capabilities. Because of the reality of the CB terrorist threat and because of the potentially disastrous consequences, a concentrated effort by both the executive and legislative branches to expedite such work would be appropriate.

The recent interagency plan to coordinate agency emergency responses to a CB attack is a welcome start in addressing the problem, but its development should receive urgent attention. Final implementation of the plan should be accelerated. This would require increased financial and managerial resources.

In the chemical area, rapid "early warning" multiagent detectors are being developed. Similar work is proceeding in the biological area, but considerably more R&D would be very useful there. In a number of fields, an optimal response and protective system requires further work. The topics of early disease detection and diagnosis need more effort; one problem is to determine as quickly as possible whether an outbreak of disease is natural or a terrorist act. **The development of lightweight protective masks that can be worn for lengthy periods of time should be emphasized, especially since it could be accomplished with current technology.** Another effort should be the development and stockpiling of vaccines, antidotes, antibiotics, and antiviral agents to combat the most likely threats (as determined by intelligence estimates). Decontarnination after an attack is another important field to emphasize. The rapid development of a real-time field device for detecting an infectious aerosol is a further need.

Improved coordination among the agencies involved in such research is desirable. In determining the direction of research and assigning priorities, participation of the intelligence community and of the Armed Forces Medical Intelligence Center is essential. An oversight board for coordinating major decisions on such research would be useful. Such a board should include representatives of military (e.g., the U.S. Army Medical Research Institute for Infectious Diseases) and civilian (e.g., the Centers for Disease Control and the National Institutes of Health) research organizations to assure maximum expertise and breadth of perspective.

Interagency Communication and Coordination

FINDING 2

There are still problems with interagency communications and coordination in counterterrorist activity and research. Interagency communication, both operationally and in R&D, has improved significantly over the past few years. However, more coordination is required for a better effort.

In years past, different agencies involved in operations against criminals did not even have a common, secure radio communications charnel. This problem has been dealt with. In the case of a chemical or biological terrorist threat, there was no coordinated plan for interagency response; now, one is being developed. In some research areas, the previous experience of parallel research efforts with minimal communication among the agencies working similar problems has been changed with the organization of interagency expert working groups. Some of these successes have been mediated by the Technical Support Working Group (TSWG), highlighted in the earlier OTA report.[4]

In other areas, existing communication efforts are poorly implemented. The 'TECSII" database, which links the Immigration and Naturalization Service (INS) and U.S. Customs terminals across the world with many U.S. Government agencies, does not seem to receive adequate attention from domestic law enforcement agencies. The database contains valuable information on a large number of foreign individuals who attempt to enter the United States and who excite suspicions of Customs or INS agents at ports of entry. In some cases, proof of criminal activity is developed, and in other cases not. A useful, organized stock of information is available but does not appear to be widely used. One of the interagency coordinating groups on counterterrorism (the Policy Coordinating Committee on Terrorism of the Interagency Intelligence Committee on Terrorism, for example) could make efforts to encourage appropriate utilization of this and other databases.

Another area of interagency confusion is reflected in a case where classification regulations significantly slowed research into a promising area of explosives detection. The company in question, pursuing computerized tomography for detecting explosives in baggage, is partly foreign-owned (a minority share is owned by Italian and Japanese interests). Research has been delayed for up to a year because, following the establishment of classification guidelines regarding the capabilities of such equipment, the company's laboratory could not be designated as a facility capable of performing classified research. The legal difficulties will be resolved, perhaps by spinning off an entirely U. S.-owned subsidiary, but valuable months of work will have been lost. Again, an interagency coordinating group should have been able to shortcut the problem.

In the area of research and development, two phenomena are salient. First, in some fields, there are redundant research projects where different agencies let substantial contracts, sometimes to the same vendors, to develop similar hardware. Second, other agencies--e.g., INS, the Secret Service, and the Federal Bureau of Investigation (FBI)-suffering from virtually nonexistent budgets for R&D, but needing to develop tools for counterterrorist and other missions, are forced to shop around for well-heeled agencies to provide funds to support these efforts.

In the field of behavioral research, as applied to passenger profiling and incident management, there appears to be insufficient coordination among agencies.

These problems should, in theory, be solved by the existence of the TSWG. This interagency committee is meant to coordinate R&D activities in this area in a way that avoids redundancies and assures that needed work gets done, even if no one agency can provide sufficient funds by itself. However, as noted in the previous OTA report, funding for TSWG has been problematic, declining by 80 percent since its inception 5 years ago. Shortage of money apparently increases the tendency to protect turf and discourages communication among the agencies doing the R&D. It also encourages scientists to use their own networks of colleagues and friends in other agencies to seek funding for needed projects—funding that should be assured and coordinated through the interagency group for such research.

[4]U.S. Congress, Office of Technology Assessment op. cit., footnote 1, ch. 1.

One area of emphasis should be the organization by cognizant Government agencies of periodic interagency conferences in areas related to counterterrorism, such as aviation security, behavioral sciences, and sensor development. Some such conferences do occur now, but need to be more regular and cover more topics.

Options

OTA presents four options for improved coordination in research among the multitude of agencies that have R&D interests in counterterrorism. There is no foolproof institutional method of assuring that a given governmental project will work optimally. Much of the result will depend on the type and quality of people assigned leading roles. Bearing in mind these constraints, Congress may wish to consider the following suggestions.

Some agencies (those of the Intelligence Community and the Defense and Energy Departments in particular) will not be interested in having counterterrorism projects that are specific to their own missions controlled or subsumed by an interagency group. But those projects with interagency applications, and there are many, should be coordinated by a central, interagency group, one that has sufficient authority and funds to run an efficient program. Further, a larger portion of the Nation's counterterrorism research should be subject to coordination by a single body than is currently the case. Now, the TSWG represents only $2 million out of over $70 million expended annually. Even if expanded to $10 million, the fraction would be only 15 percent.[5]

In considering these options, the following criteria should be applied. The coordinating group should be able to act as an effective communications channel among agency scientists. Further, agencies must take it seriously: it should be politically strong and have sufficient financial resources to overcome distrust, turf protection, and secrecy among agencies. Moreover, it should be in a position to avoid significant redundancies in research projects and to identify important areas not being researched. It should be acceptable to key agencies (the Departments of State, Defense, Energy, and Justice), if at all possible. Finally, there should be significant assurances of support for consistent funding from Congress and from the agencies concerned.

Option 1: Continue with the TSWG and its parent Policy Coordinating Committee on Terrorism as now funded, run through the Department of State, but with a large increase in funding, as now planned, mostly originating from the Department of Defense. Give the TSWG its own line item in the State Department budget.

Advantages. This continues the present institutional situation, which has worked, given funding constraints, until now. Many of the participants are familiar and comfortable with it. An increase in funding (to $10 million from $2 million, as proposed in pending legislation) should be sufficient to assure that needed projects, particularly those of research-starved agencies, are undertaken. This set-up allows decisions on research to be made by a committee made up of representatives of all the participating agencies. It is meant to assure that the large research agencies (Defense and Energy) will not dominate or gobble up the research pie.

A line-item status will help assure that other components of the State Department do not drain funds intended for the TSWG. It may also help in providing an incentive for the State Department to give more active support to the TSWG when appealing for funds from Congress.

Disadvantages. There may remain some congressional opposition to funding a research program through State, which is not a research-oriented agency. The funding may never be assured from year to year, unless strong advocates appear, either in Congress or the executive branch. Power and decisionmaking maybe perceived as tilting towards Defense, since a large share of funds will be supplied from its budget. Defense is already managing the program for State, which has limited technical expertise.

Option 2: Place the TSWG in a major research agency, such as the Department of Defense, the Department of Energy, or the Department of Transportation (now with a large R&D budget for counterterrorism). Give it line-item status.

Advantages. The Departments of Defense and Energy both have significant experience in managing R&D programs of all sizes and at all phases. Stable funding would be more likely; even if the

[5]Pending legislation has allocated $7 million from DOD funds for the TSWG.

congressional process were to fluctuate, the host agency could make up difference in lean years, since the whole program would constitute a minute part of the agency's research program.

Disadvantages. There might be distrust among other participating agencies, since the perception will be that the host agency will take the lion's share of projects. A committee may make funding decisions, but the power of the purse of the host agency might swing decisions in favor of research it particularly wants. On the other hand, the host agency may not want the program, since it may perceive that the costs of TSWG research, primarily done to satisfy other agencies' needs, would be deducted from its own in-house research.

Option 3: Replace the TSWG with a similar funding group run out of a national laboratory (within DOE) or a smaller agency with research capability. Give it line-item status.

Advantages. A laboratory would be familiar with science and engineering issues and research practices, which would help in finishing competent oversight. An operational agency would be aware of the field requirements of the equipment. In the former case, the TSWG would be somewhat removed from interagency rivalry, although subject to interlaboratory rivalry.

Disadvantages. This would place much, probably too much, power in the hands of only one participating agency, even if accompanied by an interagency oversight board. Since the TSWG would be replaced, many old players would not likely be enthusiastic, especially State, Defense, and Energy, all of which have leading roles. If the location were a national laboratory, Energy could be somewhat mollified. However, there may be resentment from competing laboratories. Further, many observers consider the laboratories more efficient at long-term research than they are at rapid prototyping, which is needed in the field.

Option 4: Replace the TSWG with a similar funding group operating out of a technical office close to the President with no direct interest in doing research itself, such as the President's Office of Science and Technology Policy, or the National Security Council (NSC), or out of a new office, following the model of the Office of National Drug Control Policy. Specifically marked money and personnel would have to be provided to any of these possible homes to run the group; piggybacking on current capabilities will not work.

Advantages. The coordinating body would be in a strong position of power (if actively supported by the White House) and thus able to arbitrate among agencies and deal with rivalries and parochial interests. A strong position would also help in eliciting information from reluctant participants and in fighting turf builders. Specifically marked funds would need to be provided, since the task of coordinating counterterrorist research is a major one, requiring the full attention of experts. If located in the White House Office of Science and Technology Policy (OSTP), the coordinating group would be likely to have strong technical input with probably no ax to grind. It could also benefit from the perception that the OSTP would be a disinterested, honest broker. This would also apply to the creation of a new office. Also, this option tight provide a good place to take advantage of existing talent to deal with the multidisciplinary needs of overseeing a highly varied program. A new office would have to receive separate research funding and control the purse strings, otherwise participating agencies would not be interested in playing. This option might level the playing field among agencies in that more weight might be given to the needs of agencies with limited R&D budgets (e.g., Secret Service, INS).

Disadvantages. The TSWG would disappear, thus irritating the same participants as in the previous option. A new ballgame of counterterrorism R&D would exist, making long-time participants uncomfortable. Major agencies might be more reluctant to play. Congress may be unwilling to fired a new agency or to increase significantly the budget for an existing office. The OSTP or NSC might be reluctant to take on the task of managing research, particularly in a narrow area.

Aviation Security

The remaining findings all deal with aviation security, although several of them have applications to other aspects of countertemorism.

Integrated Security Systems

FINDING 3

With current or near-term technology, a system combining profiling and bomb detection technology could be developed that could be expected to increase airline security.

In chapter 4, this report details an example of an explosives detection system that incorporates profiling with three different types of detectors.[6] A combined detection probability of around 0.85 to 0.90 and a false alarm rate of about 1 percent are estimated for such a system, based on estimates (probably optimistic) of the performance characteristics of individual components. The suggested system is only notional and not intended to be definitive; the goal is to present the technique of combining different technologies and to show how such an explosives detection system may be more effective and potentially less costly than reliance on just one technology. The first stage of such a system would be an "OR" gate (one that triggers further scrutiny when *at least one* component alarms), using profiling and an advanced x-ray detection device as the components.[7] One advantage of x-ray systems over the thermal neutron analysis (TNA) system (now in advanced development) for a frost stage is in the cost; x-ray systems cost only 10 to 20 percent as much as a TNA machine. There are other potential advantages, such as speed of throughput, smaller size and weight, less infrastructure needed to support the system, etc. The second stage could use a completely different technology, such as a vapor detector, and the final stage could employ a more elaborate and expensive device, such as computerized tomography or TNA.

In this system, throughput would not be a problem if profiling were done at check-in, since it would add negligible time. Only some bags (perhaps one-quarter of the total) would pass to the second stage, and far fewer still would go to the final stage, so the throughput requirement for these stages would not be stressing and probably not be an issue.[8] And, since the stage-two and stage-three equipment are only needed in small quantities, their effect on the total cost of capital acquisition would be reduced.

Again, this system is only posed as a suggestion; an optimized system might be different for each airport, depending on many factors, such as peak flow, configuration of baggage conveyors, location of check-in counters, etc. However, optimization could be analyzed for individual airports using simple programming techniques given the parameters of the detection devices (i.e., detection probability, false alarm rate, cost, rate of throughput, and possibly size and weight).

FINDING 4

The throughput rate of an individual explosives or bomb detection device is not an appropriate parameter to regulate. What counts is the throughput of the entire security system.

The FAA has mandated an average throughput rate of 10 bags/minute for an acceptable explosives detector. OTA finds that throughput is not an important parameter in itself. First, useful throughput rates vary, depending on where the device is used. Second, cost is a determining factor: if a slow device is cheaper, a solution might be simply to buy more and use them in parallel (if there is room). Third, as noted above, the placement of a device in the system determines its needed rate of throughput: one that needs to handle only a small fraction of the baggage can take much longer and still remain a useful component. Optimizing the throughput may be left to determination through systems analysis and the marketplace. One might consider specifying throughput for an entire system, but the meaningful parameter would be additional delay time introduced over and above the check-in procedure. And this would, again, be scenario-dependent, depending on the configuration of the total system.

---

[6] In addition to detecting explosives, it may also be possible to detect other components of bombs, such as detonators, power sources, or timers. Most detectors available and being researched are, in fact, explosives detectors, but some may be able to fiid the other components as well.

[7] The latter might be a backscatter machine o, a refined dual-energy system. Both these types of x-ray devices react to high-density, low-atomic-weight items, like high explosives. Or, it might be a system that looks specifically for detonators as well as for high explosives.

[8] Since only about one-quarter of the bags proceed t. the second stage, the latter equipment could take about 4 times as long as the FAA guideline of 10 bags per minute—that is, 24 seconds per bag—without causing a bottleneck, thus greatly reducing the stress on the technology. The final stage might take 20 times as long, or 2 minutes per bag.

Human Factors

FINDING 5

Widespread use of effective passenger profiling is essential for substantial improvements in airline security, especially for reducing the burden on bomb detection technology.

Profiling has been used in aviation in the United States and other countries for several years. Israel institutionalized the use of profiles in its aviation security system several years ago, but in the United States, utilization has been sporadic and not institutionalized, with the exception of a limited requirement in high-threat areas since 1986. Some U.S. carriers began using a more elaborate profile in high-threat areas in late 1986 by subcontracting with firms owned by former Israeli security personnel. To a degree, profiling can be automated. The FAA requires certain information regarding passenger travel plans to be considered in judging whether a particular passenger should receive a higher level of scrutiny. It further requires the passenger to be asked a series of questions regarding the contents of his luggage. The FAA is examining, in addition, a more elaborate system that uses a simple computer program to evaluate a number of passenger characteristics rapidly. This has not yet been mandated for airline use. In addition, several airlines go beyond FAA regulations in interviewing passengers as a basis for decisions on security processing.

However, only in the ongoing testing of an improved TNA device at Gatwick Airport near London has profiling been used as a frost screen by U.S. carriers to decide which passengers' baggage will pass through an explosives detector. This example of profiling reduces the number of bags to be inspected by a large factor. Without such a reduction in flow through the machine, it would never otherwise be possible to vet, in some fashion, all international travelers leaving Gatwick with just one TNA machine. This provides an example of profiling being employed in combination with technical security measures. In finding 3, and in chapter 4, a specific slot for profiling is discussed in the context of an integrated bomb detection system.

FINDING 6

Research on profiling and on combining profiling with security technology should be conducted by the FAA; in addition, the FAA should benefit from discussions on this issue with other agencies such as the INS, the Customs Service, and the FBI.

Several agencies have experience in profiling, applied to distinguishing terrorists and other criminals. There appears to be inadequate discussion among these agencies. U.S. airlines should be able to receive some guidance in this area from the Federal Government, rather than having to rely mainly on contracting with private security firms with Israeli experience.

There is now enough experience with airline profiling to begin examining how regulations requiring its use may be developed, at least at high-risk airports. To this end, it may be useful in addition for the FAA to consult with other Federal agencies (e.g., the INS, the FBI, the Customs Service) to learn what techniques have proven useful in the past for discovering terrorists or criminals in high-flow travel situations. It would also be of some use to examine whether additional behavioral science research into profiling would be useful. The establishment of databases on terrorist and criminal activities, with a particular view to extracting information useful for profiling, appears to be another topic worthy of research, not just at the FAA, but, at other agencies as well. In this regard, the TECSII system, developed jointly by Customs and INS, appears to be a valuable source of information that has been overlooked, to a degree, by domestic law enforcement agencies.

FINDING 7

Passenger profiling may have civil liberties implications, depending on which characteristics are used to determine who will receive increased scrutiny, and on what the consequences of increased scrutiny are. These implications should be carefully considered in developing regulations that mandate profiling.

All baggage screening violates privacy to some degree. Even more intrusive than such screening are interviews of passengers, in order to elucidate intentions, itineraries, recent actions, etc. These have become common in international air travel. There has thus far been little legal challenge to such actions on the part of airport authorities, or, for that matter, on the part of private airlines. This absence is, no doubt, due to the severe consequences of in-flight sabotage. Most people and governments

apparently consider that the small sacrifice in privacy is balanced by the resulting increase in personal safety.

Of particular legal and ethical concern is the issue that would arise if demographic characteristics of passengers are used to help determine whether or not an individual's baggage will be more carefully screened or sent through more detection devices. It is not certain that establishment of such criteria will ever be recommended by a U.S. Government agency, but some airlines in the world may do so now and the matter needs attention. Issues that bear on the legitimacy of such actions include:

- the weight given to the demographic characteristics relative to other profile information;
- the percentage of passengers flagged by demographic criteria relative to the percentage of passengers subject to increased scrutiny as a result of profiling in general; and
- the consequences of being selected for increased scrutiny.

If the only result of being selected were an additional delay of, say, 10 seconds in checking in on an international flight, most would agree that such a consequence would be negligible. On the other hand, if a passenger were to be mistreated, strip-searched, denied passage, or delayed to the point of missing a flight due to profiling based in part on demographic characteristics, then significant consequences could be attributed to discriminatory behavior. A legal analysis of these matters is beyond the scope of this report, but must be taken into consideration in promulgating regulations.

FINDING 8

If human-factors requirements, such as profiling, are demanded of U.S. carriers on international flights, imposing the same requirements on foreign carriers landing in the United States should be considered as well.

The Aviation Security Improvement Act of 1990 requires that the Administrator only approve the security program of any foreign carrier landing in the United States if the program provides the same level of protection provided by U.S. carriers serving **the same airports.**[9] *Similar* parity was specifically established in the case of the explosives detection system rule.[10] Moreover, the FAA already vets the security quality at international airports overseas that carry passengers to the United States. However, there are problems with sovereignty and sensitivity of other countries involved. The United States has no legal authority in other countries, but it does have the option of bargaining on landing rights to carriers from those countries with inadequate security systems. This leverage has already been exercised in a number of cases when U.S. authorities considered airport security in other countries to be too lax. It could also be exercised specifically in the case of profiling.

Currently, there are no profiling requirements demanded of foreign carriers. These carriers used to argue that terrorism was generally a political act against the United States, and therefore there was no threat against them, so such security measures were unnecessary. The existence of the coalition that participated in the Gulf War should invalidate this reasoning in many cases. For others, an argument can still be made that no one is immune from air piracy and terrorism, even though the United States is more frequently a target than some other nations. Further, most foreign carriers are state-supported and find it easier to pay for the extra cost of such security measures. U.S. carriers do not have this luxury, and, for small competitive margins, the added cost of security may be a serious handicap to the ability of U.S. carriers to compete successfully.

Congress and the FAA should consider options to level the field, either by demanding similar profiling security requirements of all carriers that land in the United States, or at least by examining means of compensating U.S. carriers directly for the associated economic disadvantage.[11]

FAA Research and Development Program

FINDING 9

Examining the possibilities of hardening aircraft and cargo containers to minimize bomb damage is a promising line of approach, and one

[9] Aviation Security Improvement Act of 1990, Public Law 101-604, sec. 105(k)(2).

10 54 1 *Federal* Register, 36938-36946 (Sept. 5, 1989).

[11] In earlier drafts, there was an additional OTA finding under the human factors heading, namely that FAA should place a designee of the Assistant Administrator for Civil Aviation Security on its agencywide human factors committee. FAA has recently made this change.

that should be pursued. The FAA is proceeding in this direction.

The FAA is pursuing this option with some vigor. The object would be primarily to drive upwards the amount of explosive needed to destroy an aircraft, thereby making the explosive easier to detect (another example of systems integration). The most plausible approach is to work on hardening baggage containers to allow them to direct the venting of an explosion in such a way as to minimize damage to the aircraft. Additional options would be to add liners to the baggage compartment to try to absorb or slow shrapnel that might cause catastrophic secondary damage (e.g., to hydraulic systems) and to add blow-out panels to the fuselage itself. Difficulties with liners lie primarily in the cost associated with extra weight. A problem with any modification to the aircraft is the need for recertification for airworthiness and the cost of retrofit. FAA certification personnel and airline maintenance and operations experts should be involved at an early stage, so that operationally impractical lines of research are not pursued.

OTA suggests that international cooperation, on this and related problems, would be fruitful. Such cooperation, for example, with the British, French, Germans, and Canadians, is ongoing in the counterterrorist arena and should be expanded and encouraged.

FINDING 10

There should be a closer working relationship among personnel responsible for research at FAA, personnel who set security standards in regulations, and personnel involved in operational security matters.

A major difficulty suffered by the FAA research program lies in its placement within the overall structure of the FAA, as well as its connection to the FAA Aviation Security R&D program. The Director of the FAA Technical Center in Atlantic City, NJ, reports to the Executive Director for Systems Development (within the overall FAA organization), who, in turn, reports directly to the Administrator. Within the Technical Center, the Aviation Security Research and Development Service, which conducts the program, was until recently a part of the Airports Division in the Engineering and Development Service. Thus, it was three administrative levels removed from the Director of the Technical Center. Last year, in response to both external and internal criticisms, the Aviation Security R&D program was elevated to the service level. Prior to the above change, the branch was staffed by only 13 people. Now the Aviation Security Research and Development Service has 37 employees, a distinct improvement that reflects the recent threefold increase in R&D funding. The Technical Center, and, consequently, the Aviation Security R&D program, still have no direct line relationship with the Assistant Administrator for Civil Aviation Security.

However, FAA has made other changes in an effort to open new lines of communication between the Technical Center's security work and those involved in operational security matters at FAA. Closer contact is maintained between the head of Aviation Security Research and Development Service and the Assistant Administrator for Civil Aviation Security, and a representative of the Service is resident at the FAA headquarters in Washington, DC. Further, a memorandum of understanding between the Tech Center and the Assistant Administrator, specifying areas and divisions of responsibility has been signed in March 1991. In addition, following a requirement specified in the Aviation Security Improvement Act of 1990, the Department of Transportation has created a Director of Intelligence and Security, whose missions include development of policies, planning, and the **coordination** of countermeasures to terrorist threats to transportation security.[12] These **developments are quite new, and it remains to be seen whether they will have the effect of better coordinating responsibilities in security R&D.**

Further difficulties result from the separation, both physical and organizational, of the R&D effort from those in FAA and Department of Transportation (DOT) headquarters who set policy and who are familiar with airline and security operations. The massive objections of air carriers and airport operators to the proposed mandated widespread installation of TNA devices were, at least in part, a result of policymakers' isolation from the research directors and the operational experts. On the one hand, advice from the Tech Center on the limitations of the device was ignored in overselling its ability to the public.

[12] Public Law 101-604, sec. 101, op. cit., footnote 9.

On the other hand, the large size and cost of the device were anathema to industry; it would not easily fit into many airports without costly retrofits. Closer communication among the disparate elements of FAA and between DOT and FAA could have prevented or greatly mitigated the widespread criticism of the agency for its attempt to mandate the mass acquisition of the device.

For the future, the requirements of the research program should be better grounded in the context of operational requirements. This is true, for example, for setting the amount and type of high explosives that a detector should be able to find. Past definitions of detectable quantities and types of explosives were criticized in many quarters (including OTA)[13] as not adequately reflecting past terrorist threats. This too, can be accomplished by closer contact among different FAA elements.

In fact, the FAA has moved in this direction regarding the determination of the quantity of explosives that should be detectable. It has put together a group from several agencies to determine, from empirical data, the amounts of explosives needed to destroy various types of commercial aircraft.

[13]See first report in this series, U.S. Congress, Office of Technology Assessment, op. cit., footnote 1, ch. 1.

Chapter 2

The Terrorist Threat—1991

Contents

Figures

Chapter 2
The Terrorist Threat—1991

PART I: AN UPDATE

Introduction

Radical changes in world politics since the late 1980s have produced an understandable euphoria in public opinion. The communist empire has crumbled, the Soviet Union and Eastern Europe have moved toward democracy, and an orderly transfer of power to democratic institutions has occurred across Latin America. In the Philippines the dictatorship of Ferdinand Marcos was toppled, pluralistic governments are making a comeback across Africa, and a freer political climate is developing in South Africa with the legitimization of the African National Congress and the rescission of apartheid measures.

An expectation has materialized that such favorable developments will usher in a "new world order, with positive implications for global security and prosperity. However, the record from mid-1990 to June 1991 underscores the vulnerability of the emerging reconstructed international system to continuing challenges. Threats to global peace continue. One class of threat, diverse regional struggles for local dominance, was typified by the Gulf War. Another, which often derives from that class of threat, is terrorism.

The use of both subnational and state-sponsored terrorism persists as a cost-effective, extra-legal tool in the struggle for power within and among nations. Continuing terrorist operations at both the domestic and international levels are dramatically illustrated by the upsurge of political violence connected with the Gulf Crisis and by the assassination of Rajiv Gandhi, the former prime minister of India.

This chapter examines current and future challenges of terrorism, particularly as they affect U.S. interests. The first portion of the chapter presents an overview of domestic and international terrorist events from mid-1990 to mid-1991. Two case studies follow: one analyzes single-issue terrorism, using the extreme elements in the animal rights movement as an example; the other presents the involvement of states in sponsoring terrorist activities. Concluding observations are offered in the final section.

Contemporary Terrorism—An Overview

Terrorism is not new to contemporary societies.[1] The failure of the international community to recognize terrorism as both criminal behavior and as low-intensity warfare has encouraged the expansion of terrorist activity in the last two decades. Many hundreds of terrorist groups have caused great damage worldwide; some have been exploited by state sponsors in the process. Terrorist operations have been cheap to activate and expensive to counter.[2]

The Groups

Although springing from diverse political and social roots and sustained by wide-ranging ideologies, terrorist groups share a common disposition, namely, hostility toward the moral and legal norms of the domestic and international order and glorification of violent deeds for the sake of the causes they seek to advance. They often turn to violence after frustration with the failure of legal or less extreme actions to achieve their political goals. Terrorists frequently regard themselves as morally above the

[1]There is no universally accepted definition of "terrorism." One plausible definition is the unlawful use of physical force or psychological intimidation by sub-state or clandestine state agents directed *against* innocent *targets,* primarily intended to achieve social, economic, political, strategic, or other objectives. The U.S. Department of State uses the definition contained in Title 22 of the U.S. Code, sec. 2656f(d). It defines terrorism as ". . premeditated, politically motivated violence perpetrated against noncombatant targets by subnational or clandestine agents, usually intended to influence an audience." According to the Department of State view". . . the term non-combatant target is interpreted to include, in addition to civilians, military personnel who at the time of the incident are unarmed and/or not on duty." The Department of State also considers ". . . as acts of terrorism attacks on military installations on armed military personnel when a state of military hostilities does not exist at the site, such as bombings against U.S. bases in Europe, the Philippines, or elsewhere.' See Patterns *of Global Terrorism: 1990* (Washington, DC: Office of the Secretary of State, Office of the Coordinator for Counterterrorism, April 1991). For latest sources on the definitional forms see, for instance, Yonah Alexander (cd.), *Terrorism: An InternationalResource File, 1989 Index*, and *1990 Index* (Ann Arbor, MI: UMI, 1990-1991), and *Terrorism and International Resource File, 1970-1989 Bibliography (Ann* Arbor, MI: UMI, 1991), later cited as *1970-1989 Bibliography.*

[2]For some surveys of terrorist activity, for example, Yonah Alexander and Ray S. Cline (eds.), "Worldwide Chronology of Terrorism-1981," *Terrorism: An International Journal, vol. 6, No. 2 (1982),* pp. 107-388; Yonah Alexander (cd.), *The 1986 Annual on Terrorism,* (Dordrecht, The Netherlands: Martinus Nijhoff, 1987); Yonah Alexander and Abraham H. Foxman (eds.), *The 1987 Annual on Terrorism* and *The 1988-1989 Annual on Terrorism, both* published by Martinus Nijhoff in 1989 and 1990, respectively.

legal constraints of society and government and, consequently, do not feel bound by any limits, except those they have imposed on themselves for purposes of revolutionary success.

Specifically, indigenous subnational groups, mostly acting independently but sometimes as proxies of governments, have proliferated throughout the world, seeking to achieve ideological, nationalist, or other goals (e.g., single-issue political objectives).[3]

U.S. terrorist groups represent a variety of ideologies and political and social goals. For example, among the more active current actors is the Aryan Nations, committed to white supremacy, including the elimination of Jews and other minorities. It is probably the most violent right-wing group in the United States and provides an umbrella framework to maintain ties among several similarly oriented groups. Other groups active within the past two decades have had leftist (e.g., the Weather Underground), nationalist (e.g., los Macheteros), or special interest (e.g., Animal Liberation Front) orientations.

In Europe, a multitude of ideological and nationalist groups exist. A list of the more active ones, with their principal arenas of operation includes:

- Basque Fatherland and Liberty (ETA)-Spain, France;
- Corsican National Liberation Front (FLNC)---France;
- Direct Action (AD)-France;
- First of October Anti-Fascist Resistance Group (GRAPO)-Spain;
- Provisional Irish Republican Army (PIRA)---United Kingdom;
- Red Army Faction (RAF)-Germany;
- Red Brigades (BR)-Italy; and
- 17 November Revolutionary Organization—Greece.[4]

One of the most active European groups is the Provisional Irish Republican Army (PIRA), also known as the Provos, an offshoot of the Irish Republican Army (IRA). PIRA was formed in 1969 to force Great Britain to evacuate Ulster and then to unify Ireland under a Marxist government. Acting as a clandestine armed wing of the Sinn Fein (the legal political arm of the IRA), PIRA operates in Northern Ireland, the Irish Republic, Great Britain, and also in Western Europe.[5]

Several Middle Eastern groups are of leading importance. One is the Palestine Liberation Organization (PLO). Founded in 1964 by Palestinian nationalists seeking to establish an independent Palestinian state in place of present-day Israel, the PLO serves as an umbrella organization for several constituent groups headed by Yasser Arafat, including Fatah, the Popular Front for the Liberation of Palestine (PFLP), the Palestine Liberation Front (PLF), and several others. Despite Arafat's renunciation of terrorism and his recognition of Israel, the PLO has not relinquished the "armed struggle" strategy or yet modified the Palestine charter, which still calls for the elimination of the Jewish state. The PLO is headquartered in Tunis and operates from other bases in the Middle East and around the world.[6] Most information indicates that, since the official renunciation of terror by the PLO, its terrorist activity has diminished greatly, with the exception of attacks by the Palestine Liberation Front (PLF), run by Abu'1 Abbas. The PLF appears to be a semi-renegade member of the PLO. It was responsible for the attack on the cruise ship *Achille Lauro,* and for the failed attempt to kill large numbers of civilians and tourists on Tel Aviv beaches in 1990.

A second group is the Abu Nidal Organization (ANO), often called the Fatah Revolutionary Council, a Palestinian movement outside the framework of the PLO. Formed in 1974 by Sabri al-Banna, who uses the alias Abu Nidal, ANO is also known by other names such as the Arab Revolutionary Council, the Arab Revolutionary Brigades, Black September, and the Revolutionary Organization of Socialist

[3]See, for instance, Yonah Alexander (cd.), *International Terrorism: National, Regional, and Global Perspectives (New* York: Praeger, 1976); Walter Laqueur, *The Age of Terrorism* (Boston, MA: Little, Brown & Co., 1987); and *Terrorist Group Profiles* (Washington DC: U.S. Government Printing Office, 1989).

[4]For a recent study, see, for example, Yonah Alexander and Dennis A. Pluchinsky (eds.), *European Terrorism: Today and Tomorrow* (McLean, VA: Brassey's (US), Inc., 1991).

[5]For recent studies see, for instance, Yonah Alexander and Alan O'Day (eds.), *The Irish Terrorism Experience* (Aldershot, U.K.: Dartmouth, 1991), *Ireland's Terrorist Trauma: Interdisciplinary Perspectives (New* York: St. Martin's Press, 1989), *Ireland's Terrorist Dilemma* (Dordrecht, The Netherlands: Martinus Nijhoff, 1986), and *Terrorism in Ireland* (London: Croom Helm, 1984).

[6]See for example, Yonah Alexander and Joshua Sinai, *Terrorism: The PLO Connection* (New York: Crane Russak, 1989) and "Middle East Conflict" in 1970-1989 *Bibliography,* op. cit., footnote 1, pp. 147-182.

Muslims. It aims to undermine diplomatic moves for negotiating a peaceful settlement of the Arab-Israeli conflict and to eradicate the "Zionist presence' from the Middle East. Currently based in Iraq, where it was headquartered in 1974-83, the ANO has also been located in Syria (1983-87) and Libya (1988-90). Although it has recently undergone internal friction when 100 members rejoined the PLO mainstream Palestinian Movement, and many others were murdered by Abu Nidal, the ANO is still considered as the most dangerous group in the world operating in the Middle East, Europe, Asia, and Latin America.[7]

A third Middle Eastern group, as dangerous as the ANO, is Hizbollah, also known by other names including the Party of God, Islamic Jihad, Revolutionary Justice Organization, Organization of the Oppressed on Earth, and Islamic Jihad for the Liberation of Palestine. A radical Lebanese Shi'a group, it was formed in 1983 to realize the establishment of an Iranian-style Shi'ite Islamic Republic in Lebanon and to bring about the elimination of non-Islamic presence and influences from the Middle East. Closely tied to Iran, Hizbollah operates from several bases, such as the Beka'a Valley, Beirut, Southern Lebanon, as well as from locations in Western Europe and Africa.*

A final group worthy of mention is the Popular Front for the Liberation of Palestine-General Command (PFLP-GC), run by Ahmed Jibril. This organization has been widely reported to have carried out the bombing of Pan Am Flight 103 over Lockerbie, Scotland in 1988, commissioned to do so by the Iranian Government, although the United States has now publicly accused only Libyan nationals of participation. However, PFLP-GC has taken credit for numerous other terrorist attacks in Europe and the Middle East. Press reports have indicated that this group may hire itself out for terrorist acts. It is based in Syria, and was apparently dormant during the Gulf War.

In Latin America, guerrilla movements are active in most countries. Some of these movements frequently employ terrorist tactics. Among the most dangerous is Sendero Luminoso (SL), located in Peru. Formed as a Marxist "Shining Path to the Future" in the late 1960s by Professor Abimael Guzman Reynoso, it was initially formed as an Indian-based rural rebel movement. Its aim is to eliminate the current governmental structure and replace it with a peasant revolutionary regime. Since 1986, SL has also resorted to urban terrorism, particularly in Lima.[9] In the countryside, SL has cooperated with cocaine gangs in successful attempts to raise funds and pose as defenders of the interests of the impoverished peasantry. SL's terrorist tactics include mass murders of peasants and peasants' families who refuse to join their efforts or who try to oppose them. Vicious warfare has taken place between them and indigenous tribal peoples in remote areas, as well as between them and the Tupac Amaru Revolutionary Movement, another Marxist-Leninist guerrilla group active in Peru. SL has not, as yet, become active outside Peru's borders, beyond attempts to extend some influence to neighboring Bolivia.

Among Asian terrorist movements operating during the past two decades, the more prominent have included the Liberation Tigers of Tamil Eelam (LTTE); the New People's Army (NPA) of the Philippines; and the Japanese Red Army (JRA).[10] LTTE is a national liberation movement based among ethnic Tamils in the north and east of Sri Lanka, with support among Tamils in neighboring regions of India, particularly the State of Tamil Nadu. It has been responsible for a large number of mass murders and bombings in Sri Lanka, often attacking civilians among their ethnic rivals, the Sinhalese. Many Indian officials and others suspect the involvement of LTTE in the assassination of Rajiv Gandhi, during parliamentary elections in May 1991, although LTTE spokesmen have denied the allegation.

The JRA and NPA have actively targeted American interests and citizens. The NPA was established in 1969 as the guerrilla arm of the Communist Party of the Philippines. It has organized an urban infrastructure for the purpose of replacing the Manila regime with a Maoist government.

---

[7]Yossi Melman, *The Master Terrorist: The True Story of Abu Nidal (New* York: Avon, 1987).

[8]*Terrorist Group Profiles*, op. cit., footnote 3, pp. 15-18.

[9]*Patterns of Global Terrorism: 1990*, op. cit., footnote 1, pp. 73-74.

[10]*Terrorist* Group Profiles, op. cit., footnote 3, pp. 114-130; and Frank G. McGuire, *Security Intelligence Sourcebook* (Silver Spring, MD: Interests, Ltd., 1990), pp. 109-164.

The North Korean Government has used operatives in terrorist mass murders directed at South Korean targets. Two major incidents were the assassination of several cabinet members by bombing on an official visit to Burma and the destruction of a Korean Air Lines aircraft over the Andaman Sea in 1986.

Terrorist Networks

Experience over the past two decades shows that terrorist groups thrive on collaboration across national boundaries. Shared ideologies and commitments to radical strategies, such as professed struggles against capitalism, imperialism, racism, and Zionism, motivate groups to work together on an international scale. Another manifestation of international terrorist activities is state-sponsored terrorism: the use of subnational surrogates that seemingly act independently of their governmental sponsors. State-sponsored terrorism has become a form of low-intensity conflict that states (e.g., Iran, Iraq, Syria, Libya, and North Korea) undertake when they find it convenient to engage in hostile activities without being held accountable.

The informal and formal relationships among various terrorist groups and state sponsors has resulted in a national, regional, and global framework for terror. The international character of many terrorist efforts often compounds the difficulty of identifying the initiator or sponsor of a given terrorist act. There are many examples of international cooperation in the terrorist world. The ANO has received safe haven, financial aid, training, logistical assistance, and other help, including selected operational support from Iraq, Libya, and Syria. ETA (Basque Fatherland and Liberty) received training from Libya and Nicaragua and developed ties with PIRA. Hizbollah has enjoyed extensive aid from Iran, including funding, training, weapons, and logistical and operational support. North Korea and Libya also extended help, such as logistical support. The PLO developed extensive links with many terrorist groups (e.g., PIRA) and governments. Fatah, in particular, received training and weapons from countries such as the Soviet Union, other Eastern European states, China, Cuba, North Korea, and Vietnam.[11]

An interesting aspect of terrorist networks is the formation of a "regional' framework within which like-minded groups collaborate. A case in point is the European "antiimperialist" network that consists of several Marxist-Leninist groups, such as the Red Army Faction, Direct Action, and the Red Brigades. From 1985 to February 1987 the RAF and AD established the first front. After the AD leadership was arrested, the RAF joined the RB in the second front. It folded again when the RB was neutralized in 1988. Nevertheless, there have been recent efforts to reconstruct the framework by the RAF and GRAPO. It is not surprising, therefore, that in 1990 the RAF was engaged in several proxy-operations in Germany in support of GRAPO (e.g., arson attacks and vandalism against several Spanish car dealerships in Germany) .12

Because substantial state-sponsored support of terrorist groups, particularly by the Soviet Union and Eastern Europe, has been withdrawn, and because international counterterrorist efforts are increasing and apparently becoming more successful, many subnational perpetrators will find it more critical than ever to develop stronger linkages.

Statistical Trends

The year 1990 saw the frost annual decrease (10 percent) in both local and international terrorist events since 1987.[13]

There are several reasons for the overall statistical decline of terrorist incidents in 1990. First, the apparent elimination of Soviet and Eastern European support of various terrorist groups, particularly in the Third World, has resulted in disarray among many movements. Second, the world community has increased both security measures and interna-

[11] See, for instance, *Patterns of Global Terrorism: 1990,* op. cit., footnote 1, pp. 49-76.

[12] See Yonah Alexander and Dennis A. Pluchinsky (eds.), *European* Terrorism: *Today and Tomorrow* (McLean, VA: Brassey's (US), Inc., 1991), ch. 2.

[13] These statistics are from Business R&S International, *Annual Risk Assessment 1990* (1991). Statistics on terrorism vary widely. Numerous data banks focus undomestic terrorism, international terrorism, state terrorism, terrorism in specific countries, etc. Also, interpretation of these statistics differ, depending on the body 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. Since 1979, it has issued monthly and quarterly reports 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. Other statistical databases consulted for this paper include Jaffee Center for Strategic Studies at Tel Aviv University (JCSS) and RAND Corp. materials.

tiona1 cooperation due to the Gulf Crisis and the anticipation of Iraqi-sponsored terrorist operations. Third, Syria, as a member of the U.S.-led international coalition, has become a moderating influence, as apparently was the case with both Iran and Libya. It seems these three countries applied pressures on secular and religious Middle Eastern groups to refrain from terrorist operations during the Gulf Crisis. Finally, in spite of the tensions generated by the Gulf Crisis and War, some groups were not willing to take risks on Iraq's behalf, since it appeared to be ill-positioned for its confrontation with the international coalition.

The first quarter of 1991 saw a 10-percent increase in the number of terrorist incidents, both local and international, over the previous quarter's figures, an increase that may be related to the outbreak of the Gulf War. During this period, anti-U.S. attacks increased by more than a factor of 4 relative to the same period in 1990.

Figures 2-1 and 2-2 furnish information on terrorist trends during the past few years.

Modi Operandi and Targets

Terrorist groups have utilized a wide range of tactics during the last two decades. These have included arson, bombings, kidnapings, hijackings, facility attacks, and assassinations. The terrorist arsenal comprises not only explosives and arms, such as guns, but also includes more sophisticated weapons (including antitank rockets and ground-to-air missiles).

The modi operandi of terrorist groups vary considerably depending on the motivations and capabilities of the perpetrators. In the 1970s, for example, Fatah destroyed fuel tanks at Rotterdam oil docks, murdered 11 Israeli athletes at the Munich Olympics, and attempted a missile attack against El Al aircraft in Rome. In Spain, GRAPO kidnapped the president of the Supreme Military Tribunal, assassinated the Director of Penal Institutions, and bombed a Madrid cafe, killing 8 and wounding 40. And the JRA carried out a machine-gun and grenade attack at Lod Airport, killing 26 people (including 16 Puerto Rican pilgrims to the Holy Land), attacked Shell Oil refinery storage tanks and seized a ferryboat crew and hostages in Singapore, and hijacked a Japan Airlines plane in Bombay .14

In the 1980s, subnational groups continued on two paths: sometimes targets were specifically selected and sometimes victims were indiscriminately attacked. Hizbollah bombed U.S. and French peacekeeping forces and diplomatic buildings in Lebanon, kidnaped Western citizens in Beirut, and hijacked Kuwait Airways flight 422. Direct Action bombed the American School in Paris, employed a car bomb against the headquarters of the Organization for Economic Cooperation and Development, and murdered the Chairman of Renault. In Colombia, a local group, M-19, kidnaped and subsequently killed a U.S. citizen, staged simultaneous attacks on military and police installations and banks, and seized Bogota's Palace of Justice, taking some 500 hostages, including many members of the Supreme Court (who were later killed) and the Council of State.

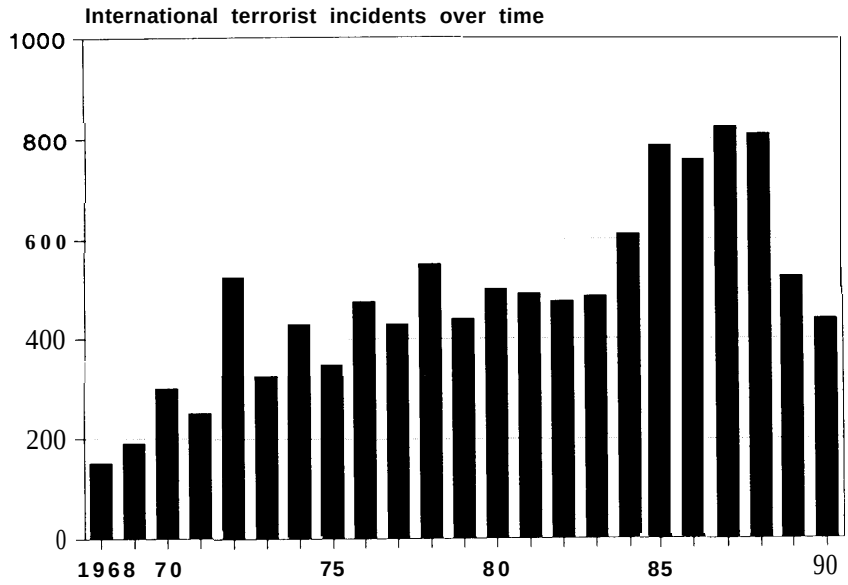
In 1990, both domestic and international terrorist groups continued to conduct their operations with similar tactics. The following few examples illustrate the nature and scope of terrorist capabilities:[15]

- Spanish Basque deputies were shot in a Madrid restaurant by ETA.
- Italian environmentalists conducted an explosives attack, damaging some French electrical utility operational equipment close to the Golfech nuclear power station.
- A house was blown up in Stepanakert, the administrative center of Nagorno-Karabakh, by unknown Armenian extremists.
- Kazem Rajavi, brother of the leader of the anti-Tehran Iranian Mujaheddin, Massoud Rajavi, was assassinated in Geneva, apparently by Iranian agents.

[14]Chronologies of terrorist events used for this paper include a variety of sources, such as press indexes; FBIS; JPRS; 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 Americans 1988);* Edward F. Mickolus, Todd Sandier, and Jean M. Murdock, *International Terrorism in the 1980s: A Chronology of Events, vol. H, 1984-1987 (Ames, IA:* Iowa State University Press); yearly reports of terrorist events prepared by the Project on Low Intensity Warfare of JCSS, such as the latest publication *International Terrorism in 1989* (Jerusalem: The Jerusalem Post, 1990); the chronologies published by the RAND 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.

[15]See, for example, BRI, *Annual Risk Assessment 1990*, op. cit., footnote 13, and *Patterns of Global Terrorism: 1990*, op. cit., footnote 1.

Figure 2-l—All International Terrorist Incidents, 1968-90



SOURCE: U.S. Department of State, *Patterns* of Global *Terrorism: 1990,* 1991.

- PIRA bombed London's Carleton Club (seriously wounding two people) and killed Ian Gow, British Conservative Party Member of Parliament in a car bomb.

By mid-1991, the sample of terrorist incidents for the current year shows similar diversity of tactics. PIRA was responsible for the mortar bomb attack against the residence of the British Prime Minister at 10 Downing Street and the bombing of crowded railway stations in London, the RAF sprayed the U.S. Embassy in Bonn with over 250 rounds from automatic weapons, and Islamic Jihad claimed responsibility for bombing the car of an Iraqi commercial attache in Ankara.[16]

The Gulf Crisis tiggered an upsurge of uncoordinated violent demonstrations and terrorist attacks worldwide, directed against U.S. or coalition targets. Many of the attacks involved incendiary devices, hand grenades, and small bombs. Most caused property damage but resulted in few casualties. The operations were usually conducted by indigenous groups that had been engaged in similar activities in the past. In claiming responsibility for some of the attacks, the perpetrators have rationalized their operations by referring to their sympathy for Iraq in the Gulf Crisis.[17]

Terrorists continue to employ a variety of methods, including assassination, destruction of property, and the murder of innocent people. They shift targets readily, making security for their enemies difficult to achieve.

The Threat to the United States, 1970-91

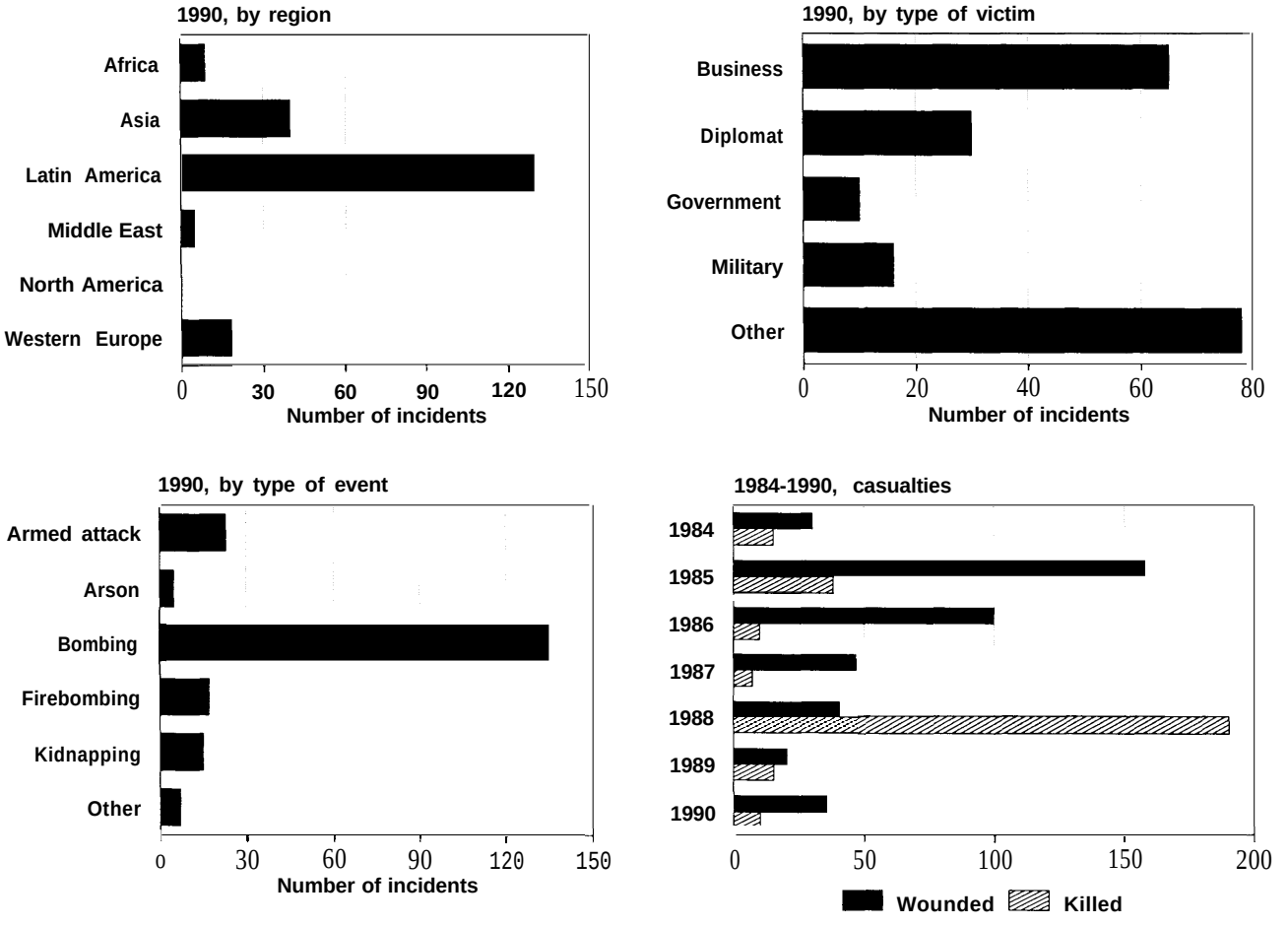
The United States is a principal target of terrorism. Not only do domestic extremist groups commit acts of terrorism in the United States, but international groups frequently do so against the many American targets abroad. However, it should be noted that international acts of terrorism have rarely occurred on U.S. soil.[18]

[16]See, for instance, BRI, Risk *Assessment Quarterly*, op. cit., footnote 15; JPRS reports; and daily press reports.

[17]Ibid.

[18]The most recent confirmed incident of terrorism in the U.S. with international implications occurred in 1983. A bombing took place in Miami that was attributed to Omega 7, a Cuban exile group. In 1989, an attempt was made to kill Captain Rogers, former commanding officer of the U.S.S. *Vincennes*, presumably in retaliation for the downing of an Iran Air aircraft over the Persian Gulf in 1988. An incendiary device caused Capt. Rogers' van to burst into flame in San Diego while his wife was driving it. She received only minor injuries. While never publicly documented, suspicions are that agents of Iran perpetrated the attack.

Figure 2-2—Anti-U.S. Attacks



SOURCE: U.S. Department of State, Patterns *of Global Terrorism: 1990,* 1991.

Domestic Terrorism

During the 1970s, indigenous and foreign terrorist campaigns in the United States resulted in 600 attacks against civilian and military targets. The success of the counterterrorism activities of the FBI and law enforcement agencies, coupled with changes in the global political environment, affected the frequency of operations domestically in the 1980s. During the last decade the number of terrorist incidents reached 200, a two-thirds decrease from the 1970s. Moreover, most of these attacks occurred in the early years of the decade.[19]

The same encouraging trend persisted in 1990 with only four events recorded, the lowest number in any year since 1970. The most dramatic event was the assassination of Rabbi Meir Kahane, the Israeli leader of the Jewish Defense League (JDL), by an Egyptian immigrant to the United States. Other events included: an abortive plot by militant "skinheads" to pump cyanide gas into a synagogue; the explosion of a bomb outside a Cuban museum in

[19]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); Samuel T. Francis, *The Terrorist Underground in the United States* (Washington, DC: The Nathan Hale Institute, n.d.); Brian M. Jenkins, "Terrorism in the United States," *TVI Journal, vol. 5, No.* 1 (1984), pp. 1-4; and FBI publications such as *Terrorism in the United States, 1989* (Washington, DC: Terrorist Research and Analytical Center, Counterterrorism Section, criminal Investigative Division, 1990).

Miami; and the arrest in Florida of individuals affiliated with the PIRA while attempting to purchase a heat-seeking antiaircraft Stinger missile and other sophisticated weapons.[20]

The evolving Gulf Crisis increased concern for potential Iraqi-instigated attacks in the United States in 1990-91. Anxiety intensified as a result of specific calls by the Iraqi leadership and Middle Eastern terrorist groups to target America. Although the fear of attacks was widespread, no incidents occurred in the United States, perhaps due to the preventive security measures undertaken by the U.S. Government and the private sector. These efforts included reduction of Iraqi diplomatic staff; close scrutiny of Iraqi and other nationals suspected of being linked to radical Arab causes; upgrading security at government and military installations; and beefing-up security procedures at airports and other commercial industries.

When the Gulf War broke out on January 17, 1991, security measures increased even further. These activities contributed to the absence of any Iraq-sponsored or foreign-related incidents in the United States linked to the Gulf War.

International Terrorism

Throughout the 1970s and 1980s, U.S. interests abroad, including cultural, economic, and military, became a major target. Generally, about one quarter of international terrorist attacks have been aimed at U.S. citizens or interests. According to one source, a total of 1,617 anti-American international attacks occurred between 1970 and 1989. Out of a total of 939 incidents internationally during January-March 1991, 104 operations were directed against Americans and U.S. interests compared to 39 in 1990 and 32 in 1989 during the same quarter. U.S. corporate targets were involved in 39 incidents, most of which took place in Latin America and Europe. This escalation was probably due primarily to the impact of the Gulf War.[21]

The United States has been the most popular single target of international terrorism. American citizens, officials, diplomats, and military officers have been victimized by both state-sponsored terrorism (e.g., Libya, Syria, and Iran) and substate groups, including Marxist-oriented (e.g., Germany's RAF), Islamic Fundamentalist (e.g., Hizbollah), Palestinian (e.g., ANO), and ideological mercenaries (e.g., JRA).

Some of the significant international terrorist incidents directed against the United States during the past decade include the following events. Although the figures cited mostly identify only U.S. causalities, in many of the incidents a large number of non-U.S. citizens were also killed or wounded.[22]

1982
- Midair explosion on a Pan Am jet bound from Tokyo to Hawaii, killing a Japanese boy and injuring 15 other passengers.

1983
- Bombing of the U.S. Embassy in Beirut, killing 17 Americans and many Lebanese.
- Bombing of U.S. Marine headquarters at the Beirut airport by a Shi'ite suicide bomber, killing 241 Marines.
- Bombing of the U.S. Embassy in Kuwait by Lebanese and Iraqi terrorists.

1984
- Bombing of the U.S. Embassy annex in East Beirut, killing two military officers.
- Hijacking of a Kuwaiti airliner to Iran, killing two Americans.

1985
- Hijacking of TWA flight 847 by Shi'ite terrorists, lasting 17 days, with the torture and killing of a U.S. Navy diver.
- Hijacking of the Italian cruise ship *Achille Lauro* by members of the Palestine Liberation Front and the murder of a disabled American tourist.

1986
- Hijacking of Pan Am Flight 73 in Karachi, killing two U.S. citizens.
- Bombing of TWA Flight 840 en route from Rome to Athens, killing four Americans, including a 9-month-old baby.
- Kidnaping of two Americans in Beirut.

1987
- Attack on a U.S. military bus in Greece by 17 November, wounding 17 servicemen.

[20] BRI, *Risk Assessment Quarterly,* op. cit., footnote 13, pp. 2-3.

[21] Ibid.

[22] This information is drawn from various chronologies available. See footnote 14 for details.

- Kidnaping of four Americans and a U.S. resident alien in Lebanon.

1988

- Kidnaping and later murder of U.S. Marine Lt. Col. William Higgins of the U.N. Observer Mission in Lebanon.
- Attacks on U.S. military personnel in Greece and Italy and American facilities in France, Spain, and West Germany.
- Destruction of Pan American Flight 103 over Lockerbie, Scotland, by an onboard explosive device killing 271 people in the aircraft and on the ground, the former from some 20 nations, but mostly Americans.

1989

- Col. James N. Rowe, a U.S. military adviser to the Philippines, was shot to death in Manila.
- Seven U.S. soldiers were wounded by a bomb in Honduras.

In 1990, similar attacks were perpetrated against U.S. interests abroad. Among the significant incidents were:[23]

- The U.S. Embassy in Lima, Peru, was car bombed, injuring three guards.
- A U.S. general with NATO was the target of an unsuccessful kidnapping or assassination attempt.

In early 1991 and particularly following the start of Operation Desert Storm, Iraq and its substate supporters called for a Jihad (Holy War) against U.S. and allied interests worldwide. Some 170 incidents were recorded against the coalition members, most of whom were Americans. For example, the U.S. Embassy in Lima was struck on January 25,1991, by an RPG-7 rocket-propelled grenade, causing only superficial damage. The Tupac Amaru Revolutionary Movement, which claimed responsibility for the incident, condemned the United States for its involvement in the Gulf and offered its militant support for the Arab people who are being murdered by U.S. troops in Iraq.[24]

Similar low-level attacks were perpetrated without any direct connection to Iraq itself. There were attacks on U.S. embassies and consulates (e.g., Frankfurt, Berlin, Sydney, Dhaka, Mexico City, Istanbul, Kuala Lampur); U.S. military personnel and facilities (e.g., Jeddah, Ankara, and Izmir); U.S. Government facilities (e.g., Voice of America transmitter compound in the Philippines); U.S. businesses (e.g., Ford, Coca-Cola, American Airlines, American Express, Holiday Inn, Citibank, Chase Manhattan Bank, and Kentucky Fried Chicken); and other U.S. targets (e.g., Mormon churches in Latin America, U.S.-Turkey Association, and the American School in Karachi) .25

Fortunately, the professional quality of the anti-American attacks connected with the Gulf War was largely primitive. The low-level terrorist operations demonstrated during Operation Desert Storm do not, however, provide any guarantees that future incidents will not be more costly in terms of human life and property. The past two decades provide ample evidence of the sophistication and deadly power of some groups, such as SL, PFLP-GC, and the RAF. The professional execution of a U.S. serviceman on March 2, 1991 in Greece by the 17 November group is a recent example.[26]

Case Studies: Subnational and State-Sponsored Terrorism

The frost two parts of this chapter provided an overview of terrorist actions. This section focuses on two case studies, which provide insights into how terrorism functions.

Single-Issue Political Extremism: Terrorism by Animal-Rights Extremists[27]

One source of terrorist acts is the single-issue political group. While only a small fraction of such groups engage in any illegal acts, in the United States, sabotage and other violent acts have been committed in the name of diverse causes, including opposition to abortion, animal rights, anger at the

[23] See, for example, JPRS Reports for 1990; cf. footnote 14.

[24] See, for instance, JPRS Reports for 1991.

[25] Ibid.

[26] BRI, *Special Report on Greece,* Apr. 4, 1991.

[27] This section borrows heavily from an edited version of an as yet unpublished Conference Report on "Animal Rights and Terrorism: Threats and Responses" held in Geneva, Switzerland, on May 9, 1991. Participants included OTA staff and a consultant and academic and operational experts in various aspects of terrorism from several nations. Although the Report reflects the Geneva deliberations, it does not constitute a consensus of the participants' views.

Internal Revenue Service, and environmental grievances. The incidence of terrorism as a whole has been quite low over the past decade, so that acts by single-issue groups now account for a significant fraction of domestic terrorism.

Differing from both traditional leftwing terrorists (e.g., the Baader-Meinhof Gang) and rightwing terrorists (e.g., the Aryan Nations) with their commitments to major political change, single-issue terrorists confine themselves to political struggle in one narrow area of focus. Single-issue terrorist groups are often less structured and organized than broadly ideological groups. Further, members are often mainstream individuals who, in other respects, do not differ radically from the average citizen. Often, some care is taken not to target people in terrorist actions. However, some of these groups occasionally do engage in assassination attempts or threats.

An example of single-issue terrorism is that related to animal-rights issues.[28] Various terrorist and criminal acts have been carried out under the banner of the Animal Liberation Front (ALF).[29] The actual degree of coordination of such activities is not clear, but attacks claimed by the ALF have occurred in the United Kingdom, the United States, and other countries.[30] The ALF opposes the use of animals in medical and scientific research, including psychological and surgical experimentation on living animals. It also generally opposes other uses of animals, such as for testing new drugs and cosmetics, for instructional purposes (especially in biology classes and in medical school), and for food, clothing, sports, circuses, and pets. To achieve their goals, ALF attacks have been made against a variety of targets ranging from medical and scientific research laboratories to butcher shops and furriers. Its tactics include theft of research animals, destruction of research equipment, vandalism, and physical intimidation of researchers and their families.

These acts have had a significant effect on biomedical research, slowing work in a number of areas.[31]

Government officials have become increasingly concerned about the activities of animal-rights groups.[32] Not only we law enforcement authorities attentive to threats to life and property, but they have labeled some of the acts of animal-rights extremists as terrorist. In 1988, the FBI included the ALF on its list of active domestic terrorist organizations. The FBI now lists the ALF as one of the 10 most dangerous terrorist organizations.

The Concept of Animal Rights-Concern for the welfare of animals goes back at least to the 19th century and has as its goal the protection of animals from mistreatment by people. Today, this broad-based movement continues among individuals and groups who are appalled by ill treatment of animals in any context. In fact, most people in the United States would probably agree with the proposition that humans have amoral responsibility not to cause needless suffering among other species.

Groups committed to such goals are commonly known as animal-welfare organizations. They act within democratic norms, using legal methods to bring public attention to barbaric acts against animals. Animal-welfare organizations have been at least in part responsible for legislation providing penalties for animal abusers and in setting norms for the treatment of animals in research.[33] They have pointed out abuses in research and have urged the discontinuation of the use of animals in testing programs for new drugs and cosmetics. In some cases, substitute techniques, avoiding the use of animals, have been developed and employed as a

[28] In addition to animal-rights terrorists, other single-issue political terrorists are active. For a brief overview see FBI, *Terrorism in the United States 1989*, op. cit., footnote 19 pp. 18-20. For bibliographical material see *Terrorism: An International Resource File* Indexes (1970-79, 1980-85,1986,1987, 1988, 1989, 1990), op. cit., footnote 19. For a recent treatment, see for instance, David T. Hardy, *America' sNew Extremists: What You Need To Know About the Animal Rights Movement* (Washington, DC: Washington Legal Foundation 1990), from which some of the information contained in this section is taken.

[29] See, for example, FBI, *Terrorism in the United States*, op. cit., footnote 19, pp. 18-20; Terry Mulgannon, "The Animal Liberation Front," *TVI Journal*, vol. *5, No. 4 (1985),* pp. 39-43.

[30] In the United Kingdom, a handbook for conducting terrorist acts has been distributed by a group claiming to be the ALF.

[31] A study on the use of animals in medical research was published by the *office* of Technology Assessment in 1986—U.S. Congress, Office Of Technology Assessment, *Alternatives to Animal Use in Research, Testing, and Education,* OTA-BA-273 (Washington DC: U.S. Government Printing Office, February 1986).

[32] See, for instance, Henry Cohen, "Brief Summaries of Federal Animal Protection Statutes," *CRS Report to Congress* (July 29, 1988).

[33] For example, Public Laws 99-158 and 99-198.

result. They have also opposed the use of animals for teaching purposes and, in fact, such use has been decreased, also in favor of alternative methods, many of them computer-based.

In recent years, some animal-rights organizations have taken extreme positions relative to those of the traditional animal-welfare groups. Some believe that animals are on an equal moral plane with humans. Within this more extreme movement, small groups of individuals have determined that violence is justified in order to further the goals related to perceived rights of animals. These groups often refer to their actions as having been carried out by the Animal Liberation Front.

Animal-Welfare Organizations and Animal-Rights Organizations-Established, traditional animal-welfare organizations include the Royal Society for the Prevention of Cruelty to Animals in Great Britain, the Society for the Protection of Animals in France, the Humane Society of the United States, and the American Society for the Prevention of Cruelty to Animals in the United States. Many countries have similar groups.

The past 30 years have seen the emergence of more extreme groups, a small fraction of whose members engage in terrorist tactics. Among groups of activists involved in antihunt protests in Great Britain in the 1960s, one faction branched out into activism against researchers. The frost animal-liberation front was formed in 1972 under the name Band of Mercy. Ronnie Lee, its founder, was convicted of violent acts against research facilities, went to jail, and was released in 1976. His group reformed as the ALF, and continued violent efforts using arson and other means to try to remove animals from research facilities.[34]

A U.S. chapter of the ALF is believed to have been organized in 1982.[35] By the mid- 1980s, the ALF had established a presence internationally. Active ALF chapters are believed to exist now in 45 countries.

The ALF has no central organization, organized leadership, membership lists, central funds, or command structure. The ALF is a flag of convenience for anyone who wants to go out and perform direct action against any form of perceived animal abuse.

People for the Ethical Treatment of Animals (PETA),[36] formed in 1980, is the largest animal-rights organization in the United States. It has 350,000 members and an annual operating budget estimated at about $8 million. PETA leaders are reported to have acted as intermediaries to the press for the ALF, including distributing a videotape of an ALF break-in.[37]

The Physicians Committee for Responsible Medicine (PCRM) works closely with PETA. Begun in the mid- 1980s, it provides the support of health care professionals to the antivivisectionist cause, which opposes any use of animals for research. The views of PCRM appear, however, to have little support within the medical community .38

Philosophical Underpinnings[39]—Animal-rights extremists are most typically motivated by philosophical beliefs based on these ideas: 1) animal rights are on a par with human rights; and 2) animals have a right to physical liberty. Since animals should have much the same rights as human beings, they conclude that one should no more destroy an animal than a child. The co-founder and director of PETA, Ingrid Newkirk, was reported to have said, "Six million people died in concentration camps, but six billion broiler chickens will die this year in slaughterhouses. '[40]

According to this line of thinking, animals should be protected from harm caused them by all human actions, ranging from a desire to consume animal products as food to the use of animals for experimentation in medical research.

---

[34] See Hardy, op. cit., footnote 28, pp. 16-17.

[35] See, for example, FBI, Terrorism *in the United States*, op. cit., footnote 19, pp. 18-20; Terry Mulgannon, "The Animal Liberation Front," *TVI Journal, vol. 5, No. 4 (1985),* pp. 39-43.

[36] For some of PETA's material see, for example, *Animal Rights 101 Workbook* (no date of publication available) and *Becoming an Activist: PETA's Guide to Animal Rights Organizing* (no date of publication available).

[37] FBI, op. cit., footnote 19, p.1 and *Nature,* April 13, 1989, p. 534.

[38] See, as an example, American Medical Association, *Use of Animals in Biomedical Research: Challenge and Response,* AMA White Paper (1989).

[39] See, for instance, Peter Singer (cd.), *In Defense of Animals* (Oxford and New York: Basil Blackwell, 1985) and Peter Singer, *Animal* Liberation, new ed. (New York: Random House, 1990).

[40] *The* Washington *Post,* Nov. 13, 1983, p.1.

Tactics-since the ALF originated in Great Britain, it is instructive to examine the tactics it has used there. In its formative period, the ALF engaged in arson and raids to achieve its objectives.[41] In 1982, the frost personal attacks with letter bombs occurred. First, these letter bombs were sent to political leaders and then to researchers. The acts were claimed by the Animal Rights Militia. There is good evidence that the ALF and the Animal Rights Militia are simply different parts of the same group.

The scale of direct action by the ALF escalated in the 1980s in Great Britain. First, there was a series of massed daylight raids in which up to 300 animal-rights activists would attack a research organization-often a pharmaceutical company. Demonstrators would tear down the wire fence, rush into the facility, grab animals and documents; by the time the police arrived 20 minutes later, they would be gone. From 1984 to 1986, there were about 10 or 12 of these daylight raids.

One section of the ALF went on to more serious terrorist activities, with car bombs first being used in 1985. The ALF started with crude explosives, but became more sophisticated. They were always placed under cars. Timed devices were often set to explode when the car was unoccupied, so most were apparently designed to blow the car up rather than kill the owners. The year 1985 was the peak of illegal activity but this included a large amount of minor activity, such as pouring glue into the locks of butcher shops, smashing windows, and setting off incendiary devices, rather than terrorism.[42]

According to one estimate, between 1985 and early 1991, there were 182 incendiary or explosive devices planted in Great Britain by animal-rights activists.[43] This number accounted for approximately 50 percent of all explosive devices planted in all of Great Britain, making it numerically a larger problem in Great Britain (i.e., the United Kingdom excluding Northern Ireland) than incidents attributed to the Provisional Irish Republican Army (PIRA). However, the majority of these devices were far less sophisticated and far less dangerous than the PIRA devices.

More recently, there has been an escalation in tactics. The use of incendiary devices by the animal-rights terrorists, which in the past were used against animal-research facilities but more frequently against shops, came to a head in late 1989. There was an attack on a department store in Guinness called Dingel's. The goal of this sort of attack was apparently to set off the sprinkler system, ruining a large quantity of merchandise. The sprinkler system in Dingel's was not operational, however. Not only did the entire store burn down, but the rest of the city block, as well. The shop has not yet been rebuilt, but the owner, the House of Frazer, has estimated that the loss was 183 million pounds. In financial terms this has probably been Great Britain's biggest act of terrorism.

Also in 1989 in Great Britain, the frost uses of high explosives by animal-rights terrorists took place. These acts appear to have been perpetrated by a small group, which had obtained a high explosive used both in military operations and in commercial applications, such as quarries. First it was used against the staff restaurant at Bristol University, where a 5-pound bomb was set off about midnight, wrecking about two floors of the building. More recently in 1990, the same explosive was used presumably by the same group in two car bombs. In one case, a passing infant was severely wounded.

According to *Science* magazine,[44] the ALF was responsible for 44 bombings and 422 violent incidents in the United Kingdom during 1989; 16 bombings and 338 attacks in 1988; and 33 bombings and 708 attacks in 1987.

Since 1982, the ALF in the United States has also been involved in illegal activities in many ways similar to those of its British counterpart resulting in its eventual inclusion on the FBI's list of terrorist organizations. In 1982 and 1983, it removed laboratory animals from Howard University Medical School in Washington, DC, and other research institutions in the area. In later years, it conducted similar raids elsewhere.

The ALF expanded its activities by vandalizing laboratories and ruining medical research records. By means of arson, a veterinary diagnostic center at

[41] See Hardy, *op.* cit., footnore 28, PP. 16-24

[42] Ibid.

[43] Ibid.

[44] *Science*, June 22, 1990.

the University of California at Davis was severely damaged. In 1989, it entered the University of Arizona's Pharmacy and Microbiology Building and another building where the Office for Animal Resources was located. It set fires and stole more than 1,000 research animals in the Arizona raid. The ALF has conducted many other raids on facilities in which animals were used for medical research. The effect of such raids and arson was to set back scientific research on cancer, heart disease, and cystic fibrosis.

A particularly well-known attack occurred in 1990, when the ALF raided the laboratories of Dr. John Orem, at Texas Tech University in Lubbock, TX. Dr. Orem had been conducting research on Sudden Infant Death Syndrome (SIDS), known commonly as ''crib death. ' The terrorists stole animals used in experimentation, destroyed laboratory records, and caused 50,000 dollars' worth of equipment damage. Dr. Orem received death threats later.

Another target of animal-rights extremists has been the U.S. Surgical Corp., which is the world's largest producer of surgical staples. These staples are essential in major operations, reducing the likelihood of surgical failure. In 1988, an animal-rights activist attempted to assassinate Leon C. Hirsch, the president of the corporation, but the effort did not succeed.

The ALF has raided meat companies and damaged butcher shops. It vandalized the cars and homes of employees of the San Diego Zoo. On several American university campuses, it has threatened scientists engaged in animal research with death or physical injury. In a few cases, animal-rights extremists planted car bombs in cars owned by medical researchers using animals in laboratory experiments. Some extremists claimed that these bombs were designed as a warning and not as killing devices.

The ALF has caused millions of dollars' worth of damage in the United States. During 1989, animal-rights extremists were responsible for numerous incidents of break-ins, thefts, arson, vandalism, and bomb threats in the United States. In addition to the direct financial cost caused by this violence, there are the additional costs borne by hospitals and research laboratories that are now required to provide enough security to deter or prevent terrorist acts. Animals in these places for scientific investigation are kept under costly 24-hour guard.

Groups identifying themselves as the ALF have engaged in such violent acts as attacking laboratories, furriers, butcher shops, and other animal-related facilities not only in the United States but also in other countries, such as Canada, Australia, New Zealand, the Netherlands, Germany, France, and South Africa.

Impact on Society-These attacks have had a significant impact on society, most importantly, on scientific progress in biomedical research. Following the ALF's position that animals should never be used for research, terrorists have delayed research, destroyed its results, caused the diversion of research funds to security measures, and caused the cancellation of at least one research program. Bills to stem lab break-ins have been introduced in Congress.

Biomedical research scientist nearly unanimously consider animals to be vital in experimentation. But animal-rights groups contend that scientists can find alternative means to conduct any useful experiments. Such objections usually refer to cellular experimentation and computer simulations as such alternates. In reply, scientists assert that, while this may be true in part, all experiments using animals cannot be substituted by these alternate means. Cellular work has, in fact, increased in recent years with the goal of avoiding the use of animals where possible, but such techniques cannot adequately imitate the biological activity of an entire organism.[45] Further, computer simulations need experimental vetification before they can be trusted, especially when human lives depend on their reliability.

State-Sponsored **Terrorism: A Case Study of Syria's Role**

It is important to assess the nature of "state-sponsored' terrorism in contradistinction to other forms of political violence ranging from single-issue political extremism to revolutionary subnational activities. State-sponsored terrorism fits under the

[45]See, for example, U.S. Congress, Office of Technology Assessment, op. cit., footnote 30.
. . . isolated systems give isolated results that may bear little relation to results obtained from the integrated systems of whole animals.

larger heading of "low-intensity conflict."% That term has been broadly, if vaguely, applied to embrace forms of warfare below the formal confrontation of national armies on battlefields. It is a category of conflict that has become more prominent in an era of weapons of mass destruction, in which the penalties of escalated hostilities loom prohibitively. Law-intensity conflict permits avoidance of those penalties. And state-sponsored terrorism recommends itself especially as a means of waging clandestine, undeclared war.

State sponsorship refers to the direct or indirect instigation and support by an established government of surrogate forces, in their exercise of psychological or physical violence, for purposes of coercion and intimidation with the goal of advancing that government's political or strategic objectives. What distinguishes state-sponsored terrorism from its other forms is the extent to which the forces carrying out the violence further the policy of an established government beyond the latter's boundaries. A terrorist group thus co-opted can be used to disrupt a target country's political stability, economic fabric, and external relations in ways which direct military confrontation could not achieve.

The compelling benefit that this long-range warfare extends to the sponsoring government, beyond a general modesty of operational investments, is the keeping of its own role hidden or the subject of ''plausible denial.' Generally, however, if a government is to be held responsible internationally for the actions of a terrorist organization, its assistance to that group has to be measured in concrete terms (e.g., direction of activities, supply of funding and armaments, permission to use national territory, and assets for training and intelligence fictions). It is the role of accomplice or accessory to the crime that constitutes concrete and convincing evidence of sponsorship of terrorism.[47]

Sponsorship becomes more direct when a government uses its own national military to arm and train a terrorist movement. When such a level of dependency is reached between a government and a terrorist organization, the government can begin to fund directly or contract out certain operations. It can regulate the internal politics or development of a group by conditioning their funding and supply of armaments on acceptance of specified tasks.[48]

On occasion, two or more governments have been involved in a particular terrorist operation. This situation derives from the nature of the international terrorist network, involving links between many governments. Cases in which a consortium of governments are involved in the conceptual and planning stages of an operation appear to be on the increase.

The case of Syria as a state sponsor of terrorism is discussed here particularly because of its important past role on the terrorist scene and the confusion about its new position in the post-Gulf Crisis period. Despite Syria's participation in the international coalition arrayed against Iraq, most experts feel it is unlikely that Syria will relinquish its terrorist weapon at home or abroad in the coming months and years. The assassination of Dany Chamoun, a Lebanese Christian leader, and his entire family on December 21, 1990, widely thought to have been accomplished by Syrian agents, is another indication that Syrian-sponsored terrorism may be ongoing.

Syria has been actively sponsoring terrorist groups and operations as an adjunct to its foreign policy in the Middle East and in the larger international arena. Over the years, Syria has itself played a role in terrorist operations, particularly against Israel, the United States, and moderate Arab regimes. Many of these operations have been also related to Syria's long-standing interest in Lebanon. To oversee these operations, Syria has setup centers in Syria itself, in Lebanon's Beka'a Valley (which is under Syrian control), and in the major capitals of Europe, where they are staffed by Ba'ath party members and Syrian security personnel who recruit additional manpower when needed from among Syrian students at universities abroad. This latter

[46] See, for example, J. Bowyer and J. Bell, *The Myth of the Guerrilla: Revolutionary Theory and Malpractice (New* York: Knopf, 1971); Richard L. Clutterbuck, *Terrorism and Guerrilla Warfare* (London and New York: Routledge, 1989); and Walter Laqueur, *Guerrilla: Historical and Critical Study* (Boston, MA: Little, Brown& Co., 1976).

[47] See, for instance, Ray S. Cline and Yonah Alexander, *Terrorism as State-Sponsored Covert Warfare* (Fairfax, *V': HERO Books*, 1986).

[48] See, for *example, Terrorist Group Profiles,* op. cit., footnote 3, pp. 29-30.

network is under the authority of the Syrian embassies, enabling those engaged in terrorist activities to pass as diplomats and to use the diplomatic pouch for the transfer of arms.[49]

Holding Palestine to be an integral part of territory taken from it unlawfully, Syria has a direct emotional involvement in Palestinian terrorist activity. Professing to be an adamant guardian of the legitimate rights of the Palestinians, Syria was the first Arab state bordering Israel to offer Palestinian terrorists a sanctuary for launching operations against that nation. In addition to providing the PLO and its terrorist elements with training facilities, expertise, equipment, and personnel, Syria also has backed its own organizations within the PLO, especially As-Saiqa.

Over the past 40 years, Syria has been involved in coups d'etat, political assassinations, and mass murder of civilians. Several examples illustrate the varieties of President Assad's tradition of terrorism:[50]

- Abed Elohab Albachri, exiled leader of the Muslim Brotherhood, was murdered in Amman, Jordan, on July 30, 1980. Two Syrian nationals were charged with the murder and were executed in Jordan.
- As an expression of opposition to the May 17, 1983, Israel-Lebanon Accord and the presence of multinational peacekeeping forces in Lebanon, Syria at least acquiesced in support for attacks on American diplomatic and military targets.[51]
- Syria was involved in attempted bombings of El Al aircraft in London and-Spain (1986).

Training-Syrian provision of military training to terrorist groups includes:

- Training camps and facilities.
- Arms transfers to terrorist groups.
- Sponsorship of mercenary terrorist groups. Syria has collaborated with and provided logistical and other support to terrorist groups that have an independent existence but followed general guidelines formulated by Syrian intelligence with regard to their targets. Among these groups are ANO, PFLP-GC, and PFLP.

Drug Trafficking and Narcoterrorism-According to the U.S. State Department:

> Syria is a transit point for illicit drugs as well as a refiner of heroin. Lebanese-produced hashish and heroin, destined for Europe and the U. S., transit Syria. Morphine base and opium from Asia enter Syria via Turkey en route to processing labs in the Beka'a Valley in Lebanon . . . Much of Syria's trafficking activity stems from Lebanon's Beka'a Valley, where Syria maintains a military presence but fails to enforce antinarcotics controls. Of greatest concern are numerous credible reports of the involvement of some Syrian officers and soldiers in facilitating the Beka'a drug trade through bribes and other corruption . . .
>
> The [U.S. Government] has reliable reports that individual Syrian soldiers and other officials stationed in Lebanon's Beka'a Valley, as well as higher-level Syrian military officials are involved in the drug trade. While this is in clear violation of Syrian and Lebanese law, there is no evidence that any of these military officers or soldiers has been prosecuted for this activity.[52]

Further, according to an interagency report on the supply of illegal drugs in the United States:

> Most of the warring factions in the country [Lebanon], as well as some known terrorist organizations, are involved in one or more aspects of the illicit narcotics trade. Sixty-five percent of the country is controlled by Syria. Periodic reporting suggests Syrian Army control over drug production in the Beka'a Valley.[53]

There have also been press reports that many of the terrorist groups sponsored by Syria in Lebanon or headquartered in Damascus derive much of their income from drug trafficking.

Summary and Conclusions—In spite of Syria's record in terrorism, can we expect anew opportunity

---

[49]See, for example, Yonah Alexander, "The Politics of Terror" (Special Report-Syria), *The World&Z* (February 1987), pp. 16-25; and U.S. Department of State, "Syrian Support for International Terrorism: 1983-86" (December 1986), Special Report No. 157.

[50]The examples axe drawn from the available chronologies on terrorism and press reports.

[51]U.S. Government, Department of Defense, *Report of the DOD Commission on Beirut International Airport Terrorist Act (Oct. 23, 1983)* (Washington, DC: U.S. Government Printing Office, 1984), p. 122.

[52]U.S. Department of State, "International Narcotics Control Strategy Report" (Washington, DC: March, 1991).

[53]U.S. Government, National Narcotics Intelligence Consumer's Committee, "The NNICC Report: 1990-The Supply of Illicit Drugs to the United States" (Washington DC: June 1991).

in the post-Gulf War period for U.S .-Syrian cooperation in combating terrorism? The question remains open. Indeed, Syria could become an invaluable ally in combating terrorism, having been a prime sponsor of it in the past, and having a strong influence over many Middle East terrorist organizations. Syria was an ally of the United States in the Gulf Crisis, and a radical change in its policy cannot be ruled out.

The Future Outlook

Future Threat Assessment

The allied victory in the Middle East drastically changed the political and military balance of power in the region. At the same time, it affected the constellation of power within and among Middle Eastern terrorist groups. For instance, the failure of secular extremists to deliver their promised attacks against members of the international coalition, Israel, and other targets has resulted in internal upheaval within these groups.

The Islamic-oriented groups may ultimately emerge as preeminent in the ''armed struggle' to regain possession of Palestine. A case in point is the Islamic Resistance Movement (Hamas), whose publicized platform asserts, "it is the personal religious duty (Fard' Ayn) of each individual Muslim to carry out this Jihad in order to bring redemption to the land.' '[54] The importance of the Harnas lies not only in its uncompromising message but in its growing popularity in the West Bank and Gaza as well as in Israel itself.

In addition to the Hamas, other fundamentalist extremist groups, such as Hizbollah, will continue to pose threats to regional stability. Not only does Hizbollah have its own agenda in Lebanon, including establishing a Shi'a Islamic State, but it also serves as a surrogate of Iran committed to eliminating non-Islamic influences and force Western interests out of the region.

Although Iranian sponsorship of terrorism dropped to 10 incidents in 1990 from 24 in 1989, and during the Gulf Crisis the number of incidents were small in number,[55] Iran continues to maintain ties with a wide variety of Moslem extremists in the region and beyond. To be sure, Iran may cooperate with the international community in regard to some specific cases, such as the release of the Western hostages (including Americans) in Lebanon, provided it obtains political or economic rewards.[56] Yet Tehran's utilization of terrorism, particularly against its domestic opponents and its support of Moslem and even of secular groups, such as PFLP-GC, is expected to remain intact.

Middle Eastern terrorists, whether secular or Moslem, will probably continue to strike not only in the region but also elsewhere in the world. Following the pattern established in the 1970s and 1980s, in the post-Gulf War period these groups will probably attempt to carry out indiscriminate attacks resulting in mass casualties. American interests, both civilian and military, will likely be affected, and the location of such attacks will not be confined to the Middle East.

Neither Middle East national groups nor regional states have abandoned the use of terrorism as a cost-effective tool. The threat has not diminished with the crushing defeat of Iraq although, for tactical reasons, revenge may take some time. As Ambassador Morns Busby, then coordinator for counterterrorism at the U.S. Department of State, recently warned: "Every war in the Middle East for the last three decades has had an aftermath of terrorism."[57]

The compounded danger is that Middle East groups-whether radical fundamentalists or secular-will make common cause with indigenous movements overseas to wage war against the West, particularly the United States. While joint operations are not likely, proxy operations, operational support, and logistical assistance are well within the realm of possibility.

Greece's 17 November is such a potential partner to Middle East groups.[58] Responding to Operation Desert Storm, 17 November carried out eight attacks, including two bombings against U.S. firms, a rocket attack on a U.S. business, and the assassination of a U.S. Air Force officer on March 12, 1991.

---

[54]Cited in Raphael Israeli, ''The Charter of Allah: The Platform of the Islamic Resistance Movement (Hamas),'' in Alexander and Foxman, The Annual *on Terrorism, 1988-1989,* op. cit., footnote 2, p. 104.

[55]*Patterns of Global Terrorism: 1990,* op. cit., footnote 1, p. 33.

[56]See, for example, *The Washington Post,* June 11, 1991.

[57]Quoted in *The Guardian* (London), Mar. 2, 1991.

[58]See, for example, Alexander and Pluchinsky, *European Terrorism Today and Tomorrow, Op.* cit., footnote 4, ch. 3.

Because no member of the 17 November group has ever been arrested during its 16-year history, little is known about its internal dynamics, composition, leadership, decisionmaking process, weapons inventory, or organizational structure. Its air of perceived invincibility creates, therefore, an operational audacity that could make this group even more dangerous and unpredictable in terms of future linkages and attacks.

The 17 November group is not the only European terrorist organization that may evolve from a minor threat to a major security problem for U.S. interests in Europe. The RAF is another potential danger, considering its history of anti-American operations.[59] Since its formation in the early 1970s, the RAF has been responsible for the deaths of more Americans than any other single European movement. During the Gulf War, it strafed the U.S. Embassy in Bonn with over 250 rounds from automatic weapons. With its infrastructure and operational capability intact, it can be expected that the RAF will pursue its "anti-imperialist" goals in the future with greater vigor. In recent attacks, its technical ability, involving difficult split-second detonations of explosives, has been manifest.

A third group is Dev Sol or 'Revolutionary Left' in Turkey.[60] A Marxist-Leninist group committed to establishing a proletarian dictatorship in Turkey, it was active in the 1970s, along with some 60 other leftwing and rightwing movements. These perpetrators were involved in over 170 anti-American operations, including the assassination of nine U.S. nationals. Although Dev Sol was neutralized by the Turkish military during most of the 1980s, it reemerged once again several years ago. Currently consisting of some 100 to 150 hardcore members operating in cells called "armed revolutionary units," Dev Sol carried out 24 low-level bombings against U.S. military, diplomatic, and business interests in Turkey, assassinated two American businessmen, and attempted the murder of a U.S. Air Force officer during the Gulf War. In claiming responsibility for the first assassination in the wake of the war of a U.S. Department of Defense civilian employee, Dev Sol warned: "We reject every agreement that fortifies the dependency on imperialism. We oppose every aspect of the economic, political, and military presence in our country."[61] This message only reinforces Dev Sol's political determination to remain an active member of the anti-American terrorist network.

Another security concern in the European context is the removal of frontier controls under the 1992 integration program. The elimination of traditional border checks will facilitate the movement of terrorists and complicate the capability of the European security forces to discharge their responsibilities. One question is whether the European intelligence services can be integrated without compromising sources of information and sensitive collection methods. These issues have taken on greater significance as a result of the Gulf Crisis. In its aftermath, the problem of a borderless Europe will pose a more acute challenge not only to the region but also to U.S. security interests.

Finally, other threats elsewhere will face the United States in the coming months and years. Regardless of the consequences of the Middle East war, terrorist dangers remain in Asia and Latin America, and single-issue terrorists will likely continue to operate in many Western nations. A major threat exists in the Philippines where a communist insurgency is ongoing. Domestic and political violence in India, the sectarian insurgency in Sri Lanka, and ultraleftist extremists in Japan might also affect American interests.[62] In Latin America, where some two-thirds of all anti-American international terrorist attacks took place and where U.S. targets were the principal foreign victims of indigenous groups in 1990,[63] violence against U.S. citizens and interests will continue unabated.

An added factor that will encourage anti-American terrorism in Latin America is narcoterrorism. It is a growing threat that combines drug criminals with political criminals. The deterioration of the situation in Colombia caused by the interna-

[59]Ibid., ch. 2.

[60]See, for instance, Henry W. Degenhardt (ed.), *Revolutionary and Dissident Movements* (Essex, U.K.: Longman, 1988), p. 377.

61 Cited in remarks by Dennis Pluchinsky in a speech on terrorism to a conference sponsored by the American Society of Industrial Security, Apr. 2, 1991, Washington D.C.

[62]*Patterns of Global Terrorism: 1990,* op. cit., footnote 1, p. 18.

[63]Ibid., pp. 18-25.

tional drug cartel over the past several years is a dramatic illustration of narcoterrorism. Indeed, terrorist groups worldwide are quickly learning that international drug trafficking offers a high-profit, low-risk way to finance their activities. These activities have become so lucrative that the drug trade has become the second largest source of terrorist funding, after state sponsorship. The United States, a leader in combating this danger, will inevitably be a prime target of these narcoterrorists.

Future Strategic and Technological Challenges[64]

Despite the latest favorable trends in the international political and military situations, as exemplified by the dramatic events in Eastern Europe and the discrediting of communism in most countries, the foreseeable environment poses three primary concerns for U.S. policy and defense strategy. Future threats-often localized in the Third World but containing regional and global security implications —will include terrorism, insurgency and revolution (often with anti-American overtones), and international drug trafficking.

Several factors make Third World countries especially vulnerable to these forms of low-intensity conflict:

- Soviet retrenchment in some regions (e.g., Middle East) and the withdrawal of direct and indirect Soviet bloc support to various terrorist groups (e.g., the PLO). This retrenchment means that the Soviet bloc will have less control over this area and, consequently, individual terrorist groups will be less disciplined and more prone to violent acts.
- The continued utilization of terrorism by some states.
- The continued existence of repressive authoritarian regimes (e.g., right and left ideologically) in Latin America.
- Pronounced ethnic fragmentation under pressure from cultural diversity and economic adversity (e.g., Africa).
- Regional conflicts that are deeply rooted and defy efforts at quick solutions (e.g., South Asia).

Future technical threats must be anticipated in order to maintain a proactive R&D policy. If currently popular explosives become too difficult to bring aboard aircraft, for example, terrorists may try different explosives or incendiaries. A frightening future prospect is the employment of weapons of mass destruction. Serious consideration should be given the possibility that subnational groups, with the direct or indirect support of some states, may turn to this tactic. It has been suggested, for example, that attempts to bring terrorism under control through national and international legislation and increased security and enforcement measures might, in fact, frustrate routine terrorist actions and spur more daring types of terrorism. Vulnerable mass targets, now available because of technological advances in contemporary society, are likely to become more attractive to terrorists.

Of course, weapons differ in terms of their characteristics and modes of actions.[65] Radiological, chemical, or biological weapons are more likely to be used than nuclear explosives. More specifically, there are no serious technological impediments to the utilization of chemical or biological agents (e.g., fluoroacetates, organophosphorous compounds, botulinum toxin). They are relatively easily obtainable, their delivery systems are manageable, and their dispersal techniques are efficient. In fact, terrorists desiring to make nerve gases themselves rather than obtain them directly from Libya, Iraq, or even the commercial market, can still find the formulas at some libraries despite attempts by some governments (e.g., Great Britain) to remove them from public access.

Once in possession of such information, a terrorist with some technical know-how could synthesize toxic chemical agents from raw materials or intermediates. In fact, many poisonous radioactive or chemical substances (e.g., Cobalt-60 or TEPP insecticides) are commercially available. They can either be bought or stolen. Covert and overt options for dispersing chemical agents are virtually limitless.

As in the case of chemical violence, biological terrorism-the use of living organisms to cause disease or death in human beings, animals, or

[64]This section benefits from as yet unpublished proceedings of two conferences on 'Terrorism and Technology: Threats and Responses. " The first was organized by the Ministry of Science and Technology of Israel and the Israel Security Research Center and held in Tel Aviv on Aug. 8, 1990. The second gathering on the same topic was held in Geneva, Switzerland on May 8, 1991, under the auspices of the Institut Henry-Dunant of the International Committee of the Red Cross. OTA staff and a consultant participated in both conferences.

[65]For sources on mass destruction threats see, for example, *Terrorism: An International Resource File,* Bibliography (1970-89), pp. 191-195.

plants—is technically possible. Many agents are relatively easy to acquire, cultivate, and disseminate.

Chemical and biological weapons, then, have many advantages for terrorists. These benefits include their low cost, the ease and speed of their production, and the fact that they can be developed by individuals without much advanced training. Weapon development requires only a minimum amount of tools and space, and equipment can be improvised or purchased without arousing suspicion. A more detailed discussion of biological weapons is presented in the following section of this chapter.

Since chemical and biological weapons could also be "weak" states' nuclear substitute for weapons, their proliferation, particularly in the Third World, is a disturbing trend. Libya and Iraq have provided recent lessons of the challenges that will confront us in the post-Gulf War period, and as noted earlier, both sponsor terrorist groups. The great danger is that if one terrorist group succeeds in achieving its goals through the utilization of mass destruction weapons, then the temptations for other extremists to escalate their operations may become irresistible.

These eventualities force us to develop adequate strategic and technological responses if future terrorist challenges are to be minimized. Because future threats will be novel, the responses of both governmental and nongovernmental bodies must be as well.

PART II: TERRORISM AND BIOLOGICAL WEAPONS

Biological Weapons: Agents and Dissemination

Biological warfare agents include living microorganisms (bacteria, rickettsia, viruses, fungi) capable of entering the human body (e.g., by inhalation or ingestion), multiplying, and causing illness or death-some of these can produce epidemics. They also include toxins produced by microorganisms, plants, or animals; and chemicals that regulate biological functions. This last category of agents (e.g., hormones, sleep peptide) has normal physiological effects in low and moderate doses but pathophysiological effects at high doses. Unlike living micro-organisms, toxins and chemical regulators only affect people directly exposed to the agent—they cannot spread from person to person.

Introduction of a specific agent or the mixture of biological agents into a delivery system (aerosol generator, aircraft spray tank, missile, artillery shell, or bomb) constitutes a biological weapon. Human delivery (e.g., a saboteur carrying a container fried with bacteria or toxin to be used to contaminate food, water, or medications) can also be utilized.

Tactics, weapons, and choice of agents will differ, depending on whether biological agents are to be used for military or terrorist purposes. In the former case, the aim will usually be to disable enemy troops so that an action may be successfully carried out with the least possible difficulty for the attacker. A fatal scourge, while fitting the requirement, may not be necessary; it may even be seen as excessive. The weapons should disperse quickly, the geographical area of interest maybe relatively small, and the time to develop symptoms should be relatively short, perhaps a few hours. The attacker may also gain an advantage if the agent can be disseminated without detection-countermeasures then become harder to effect. Finally, the choice of agent should not be one that the enemy can defeat with a vaccine or treat rapidly with antidotes, antitoxins, or antibiotics.

In the case of terrorism, there is more latitude for the attacker. Civilian populations are less likely to be immunized or protected against biological attacks as military populations may be. Nor will there likely be a nearby supply of appropriate medication. Also, the time to develop symptoms need not be short and the attack does not have to be surreptitious (although if it is, any defensive reaction becomes more difficult). The purpose, after all, is to sow terror. For this same reason, the terrorists might wish to cause mass casualties, as they do in aircraft bombings, rather than simply to disable victims temporarily, as in the military case.

Entry Into the Target

Biological weapons are usually designed to allow the selected agent to enter the human body by the aerosol route. Once in the lung, it invades the bloodstream and lymphatic and, in the case of micro-organisms, initiates infection. Similarly, drinking or eating contaminated food or beverages leads to infection by entry of the agent through the mucous membrane of the intestinal tract. Toxins may be ingested or inhaled. Most chemical regulators require the inhalation route, and little is known about the effects of their ingestion.

Inactivation of Biological Agents by the Environment

Many biological agents, especially living organisms, may be rapidly inactivated by ultraviolet light or by specific climatic conditions. However, stabilizing compounds or environment-resistant microorganisms have been developed to prolong the useful half-life of weapon agents. Further, some toxins are quite resistant to moderate heat and ultraviolet light. Also, staging attacks at night would avoid the degrading effects of ultraviolet light. Nighttime is also frequently a period of temperature inversion (warm air below dense cooler air) of the surface atmosphere. Inversion can trap an aerosoled agent near the Earth's surface, increasing the inhalation exposure time and the concentration of aerosol inhaled by the target population.

Detection of an Attack

An aerosol attack and food/beverage/medication contarnination are not normally detectable by the human senses (the agents are invisible, silent, odorless, and tasteless).

No reliable, sensitive, and specific system, whether based on mechanical, laser, electrical, or chemical detectors, is yet available to detect an aerosol attack in time to allow the target population to put on protective masks and clothing, and thus avoid inhalation and infection. This deficiency means that there is risk even from those agents that produce illnesses that can be successfully treated.

Similarly, there is no testing system in place to ensure against food/beverage/medication contamination. In some cases, attacks may be detected by finding delivery vehicles (bomblets, rockets, or bombs containing remnants of agent) or by intercepting aircraft with spray tanks, but such attacks could be planned for miles upwind of the target and go undetected.

Vulnerability of Human Target Populations

Both civilian and military populations are vulnerable to the effects of these weapons. To ensure complete protection against aerosol infection, it would be necessary for troops and civilians to constantly wear masks and protective hoods and suits. HEPA (high-efficiency particulate air) filter masks do exist that can protect against aerosols (Racal Corp., Frederick, MD). These require a battery-driven motor to ensure adequate ventilation, since the masks are bulky and require fatiguing respiratory effort to draw air through their filter systems. Masks and suits do work and are practical for short periods of time (a few hours), especially for military personnel, although they may cause a drop in ability to function effectively. It is, however, not practical for a military or civilian population to spend 24 hours a day in protective masks or suits.

Differences Between Biological and Chemical Agents

Biological weapons are difficult to detect while the attack is occurring, and there may be a long period of time between an attack and the onset of clinical symptoms of illness. Chemical weapons, on the other hand, may produce a specific odor (cyanide-bitter almonds; phosgene-newly mown hay). Rapid chemical tests are available in the field. These weapons produce casualties rapidly, giving early warning to the unaffected members of the target population and allowing them to don protective masks and suits in time to prevent further casualties.

Biological weapons can be effective in such low concentrations that attempts to detect them reliably in aerosol form by laser methods or by rapid biochemical tests have, thus far, been unsuccessful.

Targets-Tactical and Strategic

In the `military` field, biological agents may be used in tactical weapons to inflict casualties on a specific site (e.g., an airfield, aircraft carrier, missile silo, the Pentagon, the White House, the Capitol, etc.), or as a strategic weapon of mass destruction, the aim being to produce large numbers of casualties rapidly (e.g., among the U.S. and allied forces of Desert Shield, or the civilian population of a large U.S. city).

Attacks on these types of targets with biological weapons were probably possible as far back as the late 1960s (based on research done within the U.S. military offensive biological weapons program). Computer-modeled scenarios have pointed to the effectiveness of biological attacks on localized targets or large civilian populations. Livestock and plants are also vulnerable to attack. The purpose of the latter type of targeting would be to interfere with food production and damage the U.S. economy.

Possible Use by Terrorists-Availability of Technology

There has been, as yet, no major case of a terrorist attack with biological weapons. Nevertheless, terrorists have not balked at mass killing, so this possible consequence of the use of biological weapons cannot be considered to have been the principal deterrent to their use in a major attack. Such weapons may pose a risk to their users, but this can be overcome, at least to a degree, by the use of protective clothing and masks, or, in some cases, by vaccines. An advantage for the terrorists is that, in a well-planned and well-executed attack, there is less likelihood of apprehension than in case where more conventional weapons are used—they may be thousands of miles away when the first casualties occur. Such attacks also may leave no signature unless the participant terrorist group or its sponsor claims credit. It is possible that an outlaw state could utilize terrorists to deliver biological agents at a distant site.

Biological agents manufactured in a terrorist state might also be stockpiled in the United States or Europe by terrorists. They could be sent in small amounts in valises, parcels, or trunks and, over a period of months, stockpiled in major U.S. cities for later use. Since it is impossible, at present, to stop the arrival of relatively large amounts of drugs in the United States, it would similarly be impossible to prevent the arrival of much smaller quantities of living micro-organisms or toxins. Such shipments could even enter through normal shipping or airfreight routes. Alternatively, seed cultures could be smuggled into North America and the agents mass produced in clandestine laboratories in the United States or Canada.

The technical requirements for culturing micro-organisms or producing toxins for use in bioweapons are not particularly high. Most estimates are that second-year or third-year medical or microbiology students would have enough laboratory experience to prepare an agent with minimal danger to themselves. Further, some states that are suspected or known to have bioweapons programs also are known to have sponsored terrorist groups. While this does not mean that the technology for **producing bioweapons will be transferred by such states to a surrogate group, the possibility of such technology transfer, either witting or not, cannot be excluded. U.S. authorities must consider this possibility as a matter of prudent planning.**

Possible Agents for Terrorist Bioweapons

Some specific biological agents that are considered most likely to be produced by terrorists are listed and briefly discussed below.

Bacillus anthracis(anthrax)-Large numbers of organisms are required to cause the disease. If a diagnosis of aerosol exposure to B. *anthracis* is made prior to the onset of symptoms (i.e., within 48 hours of exposure) high-dosage penicillin therapy may reduce mortality, which is otherwise very high.

Use of Reynier or Anderson air samplers, containing bacterial culture plates, would allow detection of an attack prior to the onset of clinical illness in those exposed. This relatively crude, but sensitive and specific system, was used during the U.S. offensive weapons program (canceled about 20 years ago) to quantify the concentration of organisms used in simulated aerosol attacks. A diagnosis of respiratory anthrax can also be made rapidly from a blood culture and a blood smear or a fine needle aspirate of a swollen node (i.e., culture and Gram-stained smear).

As with other micro-organisms, there is a risk of lethal infection for those working with B. *anthracis* from accidental release of the agent in aerosol form during preparation for use in weapons. Immunization against anthrax (as well as the use of protective masks and clothing) can prevent terrorist casualties during the manufacture and delivery process.[66]

Francisella tularensis-This bacterium is highly infectious in aerosol form. The onset of illness is more rapid when a larger number of organisms is inhaled. The severity of the illness and the frequency of pneumonia produced are also dose-dependent. Far fewer organisms are needed to cause onset of symptoms than for anthrax. Serious pleuropulmonary tularemia has a mortality rate of up to 30 percent without therapy, but this can be reduced to a few

@B. *anthracis* is the agent that caused a large outbreak of fatal anthrax in Sverdlovsk, USSR in April 1979. U.S. intelligence believes that there were over 1,000 deaths and that the epidemic resulted from the accidental release of a large number of *B. anthracis spores* from a Soviet bioweapon production/storage facility. The Soviets continue to claim that the outbreak was the result of eating infected meat. They state that ordy 64 deaths occurred. The controversy over the nature of the epidemic continues.

percent by antibiotic treatment. The drugs of choice for therapy are streptomycin or gentamicin. Partial protection prior to exposure maybe achieved by use of a live attenuated tularemia vaccine.

Detection of exposure prior to illness or pneumonia onset is possible, but such equipment is currently not available for field use. Rapid diagnosis of mass casualties could be improved by developing better techniques (i.e., DNA probes with or without amplification of the target material by the poly - merase chain reaction). Work on such systems is in progress.

Yersinia pestis (Plague)-Aerosol exposure may cause plague pneumonia. As with anthrax, large doses are usually required to cause disease.

Early detection of Y *pestis in* clinical samples is now possible using a new Y. *pestis-specific* DNA probe. Test sensitivity could be increased by use of the polymerase chain reaction (PCR) to amplify the genetic material present. Use of streptomycin or doxycycline can reduce mortality if started before or at the onset of clinical symptoms.

Shigella flexneri-This organism or a related species could be used to contaminate water or food supplies of civilian populations. Military water and food supplies are usually safeguarded and are difficult to reach.

S. *flexneri* causes a wide spectrum of illness ranging from mild watery diarrhea without fever, to severe dysentery. S. *flexneri* and other shigella species are an attractive choice for use in contaminating food and water supplies, since only a small number of organisms are required to cause infection. S. *dysenteriae* (Shiga bacillus) is capable of causing extensive epidemic disease. This organism caused an epidemic in Central America in 1969 involving 500,000 people and had an unusually high mortality rate. With moderate infectious doses, shigellosis (dysentery) is a self-limited disease with a limited mortality. Doxycycline prophylaxis has been shown to be effective against this organism in field trials in military units. An oral vaccine for shigella species is under development. Several options exist for treatment, among them ampicillin and sulfamethoxide. Quinolone (e.g., ciprofloxacin) antibiotics are effective against shigella dysentery and also have activity against dysentery produced by Campylobacter jejuni and Salmonella infections. However, they may have negative side effects for children and early adolescents. The broad activity of the quinolones against the major causes of bacterial dysentery allows for rapid institution of therapy without the need to wait for culture results.

Salmonella species-Salmonella may be used to contaminate food, water and other beverages. Large numbers of organisms (10^6 to 10^9) must be ingested to produce illness, so contamination must be massive. *Salmonella typhi* causes typhoid fever. The incubation period after ingestion varies with the dose (typical numbers: 10^5 organisms-9 days, and 10^9 organisms—5 days; the range can be extended, depending on the state of the host's defenses). Therapy with, for example, chloramphenicol, amoxicillin, or ciprofloxacin usually leads to resolution of fever and other symptoms within several days. Salmonella organisms are not ideal agents for use by terrorists because they require a large ingested dose to produce disease, and because effective therapy is available. Salmonella species are included as threat agents because of evidence of prior production or use by terrorist groups (e.g., Order of the Rising Sun, a U.S. fascist group in the Midwest, and Rajneesh cult, Oregon). These events are described in a following section.

The following agents are toxins, not organisms. They cannot cause epidemics, and only affect persons directly exposed:

- Botulinum toxin-Botulinum toxin can be harvested from anaerobic cultures of *Clostridium botulinum.* The toxin can be used as an aerosol or for the covert contamination of the food and water supplies of the target population.

  Administration of polyvalent (A,B,E) antitoxin at the onset of symptoms, and to asymptomatic individuals exposed to the aerosol, may decrease rates of sickness or death. Several vaccines are undergoing evaluation, but none is available for large scale use.
- *Staphylococcus enterotoxin* B—This organism can be used in aerosol form. The toxin may cause severe asthmatic-like respiratory distress, pulmonary infiltrates and fever within hours of exposure. The disease is generally not fatal.

Biological Weapons of the Future

Terrorists are unlikely to have access to these future weapons unless they are supplied by a state with an advanced offensive biowarfare

program. Current weapons are crude relative to what is possible with the use of advances in molecular biology and recombinant DNA technology. These suggestions, are speculative and, even if feasible, would require years of careful work with state-of-the-art technology.

The following are some of the more frightening possibilities:

- Production of hardened agents resistant to the environment-genes may be inserted into the genome of an infectious agent that render it resistant to ultraviolet light, temperature, moisture and other environmental factors that currently adversely affect the effective half-life of the organism. Such alterations would make a more efficient weapon agent.
- Production of highly lethal and infectious agents-converting a highly infectious organism, like *F. tularensis* (tularemia) into more rapidly lethal agents by inserting genes for lethal toxins into the genome.
- Production of large amounts of toxins and regulators—genes for toxins that are in limited supply could, at least in principle, be inserted into the common stool organism, *Escherichia coli.* Similarly, large amounts of peptide or protein regulators (i.e., sleep peptide, tuftsin) could be synthesized for weaponization.

Biological Agent Selection by Terrorists

The microbiological skill and the size and type of equipment available to a terrorist group will determine, to some extent, the agents that would be weaponized and utilized. Some analysts (i.e., from the Armed Forced Medical Intelligence Center) think that terrorist groups, whether state-sponsored or not, would select and use the same types of biowarfare agents. These would most likely be living bacteria such as B. *anthracis* (anthrax), *F. tularensis* (tularemia-rabbit fever), *Y pestis* (plague), and Shigella (dysentery), and toxic agents that are relatively easy to manufacture (e.g., botulinum toxin, *staphylococcal enterotoxin B).* Although a terrorist group might recruit Ph.D.-level microbiologists and have a well-equipped clandestine laboratory (i.e., analogous to drug manufacturing laboratories in the Colombian jungle), it is unlikely that they would attempt to weaponize highly infectious and lethal agents like the hemorrhagic fever viruses, nonlethal viral agents like Venezuelan Equine Encephalitis, or Histoplasma capsulatum, a fungal agent. Smallpox is an unlikely agent since there are only two sites in the world where cultures of *variola* (smallpox) exist and violation of these sites could be detected and thwarted.

Protection for the User

The first level of protection would be appropriate protective suits and masks, which are in commercial production. This would be of use to a terrorist delivering a weapon and for military applications as well. If technically advanced, the producer of such weapons could develop a vaccine to immunize its soldiers and civilians against the carrier organism (i.e., *F. tularensis or C. burnetii)* or the toxin of choice. In this way, the producer could protect its army and civilians against the organism. The targeted group would have no time to produce a vaccine and use it before it sustained a large number of casualties.

Infection of other species (i.e., cattle, rodents, domestic animals) or spread to other neutral countries might be a major problem with the use of such agents in war or for terrorist attacks. Such problems would have to be taken into account by any state or sub-national group considering use of biological weapons.

Why Have Biological Weapons Not Been Widely Used by Terrorists?

There has been much speculation as to the reasons for the absence of use of these weapons, considering their effectiveness and relatively low technical requirements. Analysts have suggested the following possible explanations:

. Terrorists are familiar with things that go ''bang' and are able to achieve their objectives with the use of explosives and firearms. Since current, familiar methods appear to work, there is no need to change.[67]

[67]The idea that terrorists are satisfied with current methods may have to be altered if better security thwarts the use of bombs, rockets and small arms. In addition, state-sponsored terrorists maybe called upon to inflict large numbers of U.S. civilian and military casualties in support of a power at war with the United States. Use of biological agents is an escalation which can lead to an increased number of fatalities or sick personnel, whose care would deplete the logistical resources of the U.S. military.

- Terrorists may fear that they will alienate their supporters by use of biological weapons to produce large numbers of fatalities (e.g., tens of thousands) in a civilian population.
- Terrorists may fear that successful use of such weapons may lead to an extreme response by the target country that would result in many terrorist casualties and destruction of their group.[68]
- Terrorists are fearful of biological weapons and are unwilling to work with them.
- Terrorists may be under the control of sponsoring countries or groups of financial benefactors. Use of such weapons may be currently prohibited by these support groups.
- Terrorists may be awaiting a successful first use that leads to an important positive result. A successful use could result in "copy cat" attacks.

These suggestions are speculative; there may be other reasons that terrorists have not yet taken the bioweapon route. None of the above proposed reasons provides a guarantee that there will be no such attacks in the future.

Advantages for the terrorist of the use of biological weapons:

- Creation of fear and terror among the civilian population or military of the target country. The target government may be seen as unable to protect its citizens. Severe repressive measures taken by the target country may cause further governmental instability.
- Disruption of the economy of the target nation.
- Infliction of military casualties to weaken target forces that are in combat against the sponsoring state.
- Ability of terrorists to escape before illness begins in the target population, due to the invisible nature of the attacks and the time delay before onset of symptoms.
- Production of more terror, disruption, and casualties than conventional weapons.

Past Occurrences

A number of incidents related to threats, preparation for use, or actual use of biological and chemical agents by terrorists, are on record. These suggest that future use of these agents cannot be excluded since they already have been used or proposed for use in the past. There have been many more threats to use these agents than known preparation for use or actual use. Some of the incidents with actual evidence of terrorist group possession of an agent or its use are listed below:

- 1972—United States. Members of the Order of the Rising Sun were found in possession of 30 to 40 kg of typhoid bacteria cultures for use against water supplies in major Midwest cities.
- 1980-The Baader-Meinhof gang of Germany was discovered to possess a *Clostridium botulinum culture* and a home biological laboratory in a Paris apartment.
- 1986-Rajneesh cult in Oregon. *Salmonella typhi* (typhoid) were allegedly used to contaminate salad bars in local restaurants to influence the outcome of a local election. Seven hundred and fifty cases resulted.

Many threats have been made to poison municipal water supplies, food, and pharmaceuticals by terrorists with political, social, and religious motivations, as well as by criminals (extortionists), disgruntled employees, and (possibly) mentally disturbed individuals.

Terrorist groups most likely to use biological weapons may have one or more of the following characteristics:

1. A large base of popular support that they are not concerned about alienating.
2. A history of large-scale violence with high numbers of casualties per attack.
3. Prior use of sophisticated weapons.
4. State sponsorship

Terrorist groups that have some of these characteristics include the Japanese Red Army, Red Army Faction, U.S. white-supremacist groups (Aryan Nations), Hizbollah, and the Abu Nidal Organization.

U.S. Defense Against Biological Weapons

An overview of defensive measures that U.S. military forces and the civilian population could use during the next few years is presented in this section. These measures are possible, but have not yet been

[68]However, such fears have not been inhibitory to terrorists responsible for mass casualties (e.g., Hizbollah's attack on the Marine barracks in Beirut and the bombing of several jetliners, including Pan Am 103 over Lockerbie, Scotland in December 1988) in the recent past. Despite the large number of casualties, the perpetrators have thus far escaped unscathed.

rigorously tested in the field, implemented, and presented with appropriate training to our military forces or civilian populations. Options for improving the U.S. defense against bioweapons are also given.

Pre-attack Intelligence

Pre-attack warning is possible through intelligence. Terrorists associated with a sponsoring state are likely to use agents in the bioweapons arsenal of that state. The choice of agents available to unsponsored groups is limited to those listed and discussed above, and possibly a few others not listed because their characteristics make them unattractive offensive weapons.

Tracking known terrorists and intercepting suspicious individuals and groups moving from country to country offer some hope of preventing an attack.

Attempts by unsponsored terrorists groups operating in the United States might be detected by monitoring microbiology equipment and culture orders from noninstitutional buyers. Some attempts by individuals to acquire cultures of potential biological agents have been intercepted by such surveillance. It is unclear as to whether similar surveillance related to the purchase of laboratory equipment is in force.

Sale of cultures and equipment to individuals or groups of terrorists or terrorist suspects could be prevented.

Physical Protection

Long-term physical protection for civilians or military targets is not available at present. Collective protection for buildings using air intake biofilters (HEPA filters) is feasible, but no plans are in progress to facilitate this intervention.

Individual protection by use of light-weight masks on an almost continuous basis is not now possible because the current commercially available masks are not adequate to prevent aerosol infection. Hoods and masks used for contact with highly infectious patients at research centers are heavy and bulky and require a battery-driven motor to facilitate air movement into the mask. These masks are costly ($650) and the batteries require replacement and recharging every 8 to 16 hours. They are, however, effective in preventing aerosol infection. Research to produce comfortable, light-weight masks with similar effectiveness should be supported with a high priority. **At present, physical protection is the best generic defense against living organisms and/or toxins.**

Masks in current use by our military forces will protect against biowarfare and chemical agents. These masks, however, can only be worn for brief periods. Evacuation to an unexposed area and decontamination would be necessary before removal of protective clothing would be safe.

Detectors

Rapid, portable detectors are not available for living agents or toxins. Human illness will be the first sign of an attack. The air breathed by people concentrated in a specific area or building could be monitored by deploying Anderson or Reynier air samplers with culture plates that will grow aerosoled *B. anthracis* (anthrax), *F. tularensis* (tularemia) or *Y pestis* (plague). The cultures would have to be changed several times a day to pinpoint the time of an attack. Such detection after the attack and before human illness occurs would allow use of pre-illness treatment and could limit casualties.

Prior attempts to develop a detector that utilized a large volume air sampler and a generic test for living agents or toxins were unsuccessful. The detectors developed were too sensitive and nonspecific (i.e., there were too many false alarms). These detectors were designed to warn of an attack in time to put on a protective mask. Because of the frequent false alarms that triggered mask usage during tests, the detectors were never manufactured in large numbers or deployed.

Detection of the attack hours later and prior to the onset of illness, may be more successful than attempts to rapidly diagnose an attack in time to put on a protective mask.

Medical Defense

Pre-attack Cataloging of Epidemics—It would be useful to record all epidemics occurring worldwide. The causative agent, area of the world, symptoms and signs, mortality rates, and total number of cases should be recorded. Epidemic data should be collected for each country or region. Serological surveys in countries of interest are also useful, since they further catalog subclinical epidemics. Background natural disease data are helpful for deciding if an epidemic occurring in a specific

area of the world is natural or due to a biological attack.

It may be possible to develop computer algorithms that could utilize epidemiologic data to help give an assessment of whether an epidemic is a natural or man-made disease. The epidemiological characteristics of a biological attack are listed below. These would be compared by the algorithms with the data from a suspicious outbreak of disease.

Epidemiological Characteristics of a Biological Attack-A successful attack will appear as a point source epidemic (i.e., a large number of ill patients appearing at neighboring medical facilities over a brief time interval). A bioweapon-caused epidemic may have some of the following characteristics:

1. a record number of cases;
2. a high attack rate;
3. a high rate of very severe illness;
4. a large percentage of cases with lung involvement;
5. sick or dead animals in the area;
6. disease confined to those who were in a specific area at a given time;
7. presence of more than one disease-producing agent;
8. presence of an agent that is not normally an epidemic problem in the area where the attack occurs (e.g., respiratory anthrax in Washington, DC);
9. detection of the aerosol device (i.e., bomblets or other means of dissemination).

The maintenance of a corps of experts is important to the ability of the Nation to defend itself against potential biological attack.

Specific Diagnosis

Clinical symptoms and signs, routine laboratory, and imaging methods (x-ray, computerized axial tomography, nuclear magnetic resonance imaging) can be used to narrow the list of possible causative agents of an outbreak to a manageable number. Clinical samples of body fluids or tissues can be collected from ill or dead patients, and tested to provide rapid diagnosis and characterization of the causative agent(s) or toxin. Rapid laboratory diagnosis of specific infectious agents can be accomplished by the following types of approaches:

1. antigen-capture using ELISA,[69] DNA probes, or DNA probes with the target genetic material amplified by the polymerase chain reaction;
2. bacterial or viral cultures;
3. microscopic examination of tissue by special stains, electron microscopy and immunofluorescence; or
4. detection of a specific antibody within 3 to 4 days of the onset of illness.

Therapy

Specific Therapy—Selection of an antimicrobial drug is best if the agent and its sensitivity profile are known. This could be rapidly obtained by clinical and routine laboratory methods.

Multiple drug and therapeutic trials-If the agent and/or its sensitivities remain unknown, then multiple drugs may be given to most of the patients while small groups of patients are treated with only one drug. The drug giving the best clinical response could then be used to treat all patients and the ineffective drugs discontinued. This strategy was used in the Legionella pneumonia outbreak and rapidly identified erythromycin as the most effective drug.

Other Defensive Measures

Warning—A central authority could collect detailed information regarding an outbreak and issue warnings to military and civilian groups. This would include information regarding prophylaxis and therapy.

Care—The number of available intensive care and support beds as well as specialized medical treatment personnel could be cataloged and kept updated.

Prophylaxis—Antibiotics could be administered when appropriate (i.e., doxycycline for *F. tularensis or Y pestis).*

Vaccination-Since vaccines (of varying effectiveness) exist for *B. anthracis,* Y *pestis,* and *F. tularensis, their* adminstration could be initiated among a group at risk if immunization had not been started prior to an attack.

[69] ELISA stands for enzyme-linked immunospecific assay. The ELISA assay is a standard test for agents (micro-organisms or inert chemicals) that cause antibody reactions in larger organisms, generally humans.

Stockpiling—Antibiotics, antifungal, antiviral, and vaccines and antitoxins could be procured and be readily available for a potential target group.

Decontamination-Aerosoled bacteria such as B. *anthracis, Y pestis* and *F. tularensis* do not usually adhere to clothing or skin in high enough concentrations to create a problem of secondary aerosol. Since there will most likely be no sign of an attack for 1 or 2 days, most bacterial agents remaining in the environment will already have been inactivated or diluted. A safe approach is use of soap and water and a change of clothing after an attack has been documented. Enspor can be used to decontaminate skin and clothing for B. *anthracis if* clothing changes are not available. Dilute bleach 1:5 or 1:10 is also useful for decontamination of *B. anthracis* and viral hemorrhagic fever agents.

Improving U.S. Defenses Against Biological Attacks

It is important to develop vaccines against biological agents most likely to be used by terrorists or states against U.S. targets. To do so first requires information and gathering by intelligence agencies and analysis by experts including those at the Armed Forces Medical Intelligence Center (AFMIC) at Ft. Detrick, MD. Beyond the obvious information on construction and operation of suspect research facilities abroad, attention needs to be paid to noninstitutional purchases of cultures and laboratory equipment that could be used to produce biological weapons. Coordination with foreign intelligence agencies could be employed to obtain information about specific state-sponsored terrorist groups. This is already being done to a limited extent. Continued surveillance of foreign bioweapon programs is necessary so that threat lists of weaponized agents remain current. The U.S. should also continue surveillance of nations suspected of providing states with an active offensive bioweapons program with laboratory equipment and scientists for production of such weapons. To improve border controls, U.S. Customs officials could be trained to recognize biological weapons to the degree possible.

Decisions on the direction of research to pursue should be coordinated among the intelligence agencies, who analyze likely threats, and the military (USAMRIID) and civilian researchers (e.g., at the National Institutes of Health and the Centers for Disease Control) responsible for developing vaccines and working on other related research, such as early detection and diagnosis of biological attacks. An interagency oversight board composed of the above participants, would be a useful device to assure efficiency in research and to assign priorities.

Research and Development of Equipment for Physical Protection and Detection

Protection. A well-supported program for research, development and testing of motor-driven and other types of *biodefense* mask/hoods should be initiated. A mask that is light-weight, comfortable, tolerable for prolonged periods, and effective against toxins and biological agents should be the major goal of this program. Filter systems for the protection of buildings and other collective shelters are also important.

Post-attack pre-illness detection. Development of air sampling detection systems should be supported. Even detection of an attack after inhalation, but prior to the onset of symptoms, may result in the saving of many lives by initiation of early therapy.

Diagnosis and treatment. A computer database should be established to store epidemic disease information. This database could be used to help determine whether an epidemic in a specific area of the world is natural or man-made.

Tables and algorithms for the differential diagnosis of epidemic diseases using symptoms, signs, laboratory work and imaging studies, should be provided to physicians. Laboratories dedicated to perform rapid diagnostic tests for the identification of causative agents should be established near the attack site or at an accessible central location in the U.S. or Europe.

Antibiotics, vaccines and antitoxins should be stockpiled in high threat areas.

Vaccines for the major threat agents should be improved, tested, and then administered to those at risk.

Decontamination methods and useful disinfectants should be developed and tested against the major threat agents. This has only been done on a limited basis.

Pre-attack disaster planning should be done. This should include cataloging available medical personnel, intensive care beds, respirators and dialysis machines in the threat region, and in back-up hospitals outside the region.

Summary

Currently, U.S. targets are Vulnerable to a biological attack. Present medical defense is reactive, designed to limit mortality after the attack has occurred.

No adequate long-term physical protection against aerosoled agents is available for soldiers or civilians. Stockpiles of drugs and vaccines being held for these groups may not be adequate. No program of pre-exposure vaccination or antibiotic use has been implemented, except in limited circumstances during the Gulf War. The principal defense against a bioweapons attack by terrorists or a sovereign state consists of identification of the attack as man-made, diagnosis of the causative agent(s), and initiation of specific therapy.

More coordination among military and civilian agencies would lead to a more effective **program of research, particularly in areas related to vaccine development and early detection and diagnosis of agents. The development of effective vaccines against most likely threat agents, such as anthrax and botulinum toxin, should be given high priority.**

A physical defense in the form of effective, light-weight masks that could be worn for long periods of time is not available and has had a low priority. It would be important to have such hood/masks available in the event that bioweapons are used by terrorists or terrorist states. Antimicrobial drugs, vaccines and antitoxins effective against the threat agents should be stockpiled in threat areas. Improved intelligence is required to provide the United States with information that would allow prevention of a planned biological attack.

Chapter 3

Interagency and International Communication and Cooperation

Contents

Chapter 3
Interagency and International Communication and Cooperation

INTRODUCTION—EXAMPLES OF PROBLEMS

About 25 U.S. Government agencies deal with aspects of terrorism.[1] They are represented on the Policy Coordinating Committee on Terrorism, its technical subcommittee, the Technical Support Working Group (TSWG), and other interagency working groups. Coordination of activities among these participants has improved over the last several years, at least in part due to the availability of the TSWG as a forum. This chapter deals with problems of assuring adequate communication and coordination in the fight against terrorism.

Examples of difficulties in communication and coordination extend over a multitude of areas, from the relatively straightforward matter of exchanging information on current research or on terrorist organizations and threats to crisis coordination. OTA has not performed a detailed study of all aspects of interagency communication among the 25 (or so) government agencies that participate in counterterrorism work. However, during the course of the project, OTA has become aware of a number of problems, past and present. This chapter will provide examples of these problems. Some have been successfully resolved; others have not. Following the exposition of examples, which indicates the scope of the problem, OTA presents a series of options for improving interagency coordination for Congress to consider. In addition, there is a brief discussion on international coordination of counterterrorism R&D.

Interagency Exchange of Information

Some difficulties in communication simply involve red tape. During the course of this study, OTA staff were asked on two occasions to facilitate transfers of R&D information between one agency and laboratories belonging to another. It was not that the information was otherwise unavailable to the requester, but it was felt that due to lengthy bureaucratic procedures, going through established channels would delay information transfer by months.

There are problems regarding the dissemination of vital data of relevance to terrorism. A useful and interesting source of information, the TECSII database, is managed by the U.S. Customs Service and the Immigration and Naturalization Service (INS). It contains information, such as description and passport number, regarding individuals who may have excited suspicions on the part of Customs or INS agents when they presented themselves at a U.S. port of entry. Some may have been found carrying contraband, others may have violated other laws, and still others may have matched a suspicious profile, based on their recent travels or on other factors.

This database is available to various government agencies. However, only a very small number of terminals connected to TECSII are available to the agency with chief responsibility for domestic counterterrorist activities, the Federal Bureau of Investigation (FBI). Further, this source of information does not appear to be frequently accessed by the FBI, even during time of increased international tensions, such as during the period prior to the Gulf War in late 1990 and early 1991. True, this source of information is limited: no one who does not appear at a port of entry is included. Nevertheless, the database may contain much valuable information, particularly at times when there is reason to think that an effort may be underway to introduce terrorists into the United States.

Interagency Arguments

Another category of communication difficulties involves turf protection and institutional disputes among agencies. On one occasion, two different agencies were funding closely related research by the same contractor into explosives detection. The two agencies had different applications for the technologies, and, consequently, different specifications for a workable system. One agency ran a test on

[1] See 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), app. E for a listing of Federal participants in counterterrorism R&D.

a prototype that did not yield very favorable results. The second agency had run tests on similar equipment that looked significantly better, at least for that agency's purposes. As a result of the first agency's negative results, however, the research program of the second agency was nearly canceled by higher officials. This eventuality was averted but the upshot was a bad feeling between the program monitors of the respective agencies that became counterproductive. Fortunately, this dispute was resolved fairly quickly, but the fact that it occurred at all (in spite of the existence of the TSWG, which should have provided a natural path of communication among the individuals) is disturbing. This episode represents a serious problem of coordination among agencies involved in related research.

Turf problems, now happily resolved, were evident in another arena. The Federal Aviation Administration (FAA) is responsible for overseeing security procedures at U.S. airports. Some regulations require the display of identification badges by all personnel in protected areas at airports, particularly those areas with access to aircraft. This is to facilitate the detection of unauthorized personnel in those zones. However, the Customs Service considered that Customs officials in uniform were not required to obey such regulations. The problem, from a security point of view, is that a malefactor could conceivably obtain a reasonable facsimile of such a uniform, and would then be immune to challenge by airport authorities or local police. The refusal of Customs officials to display airport identification led, at least on one occasion, to a confrontation, with guns drawn, between a Customs agent and a local policeman.

This problem has since been resolved by discussions at high levels among leading officials in the responsible agencies. However, matters should not have been allowed to deteriorate to that point.

Classification Issues

Another example of a snafu in interagency R&D coordination involves Imatron Corp., the manufacturer and developer of a promising device to detect explosives—a rapid computertized tomography machine. Imatron performed some tests in late 1990 under contract with the FAA. The results appeared interesting and deserving of more rigorous evaluation. However, during this period, classification guidelines were promulgated by the Department of Transportation that labeled information on the effectiveness of potential explosives detectors as ''confidential. ''

A problem then arose because Imatron has some foreign minority shareowners (Italian and Japanese). Even though the company is over 50 percent U.S.-owned, foreign participation was enough to prevent Imatron's laboratory facilities from being designated as capable of handling classified data. Imatron has had to cease testing and other related work for the FAA until the problem can be resolved. The legal solution, spinning off an entirely U.S.-owned subsidiary to do the classtified work, will take months to accomplish, resulting in months of time lost.

In addition, there are some examples of redundancy of effort in some lines of research applicable to counterterrorism (and to counternarcotics). One case is the existence of several projects in different agencies developing the same technology (using relatively high-energy garoma rays) to examine large cargo containers for contraband, including narcotics, weapons, or explosives.

The existence of the TSWG has reduced the incidence of this type of duplication, but has not eliminated it. The TSWG tried, on one occasion, to assemble an updatable database of relevant R&D progress. The availability of such information would make such redundancies of effort considerably less likely. However, due to limited funding, this database was never set up.

OTA considers the establishment of an interagency database on the state of the art in technology and R&D applicable to counterterrorism to be an important part of the development of adequate coordination of the Nation's counterterrorism effort.

Scrabbling for Funds

Some agencies with limited R&D funding resources are currently forced to seek funds from more affluent agencies in order to pursue research projects that they feel are essential. An example is the INS, which has only $400,000 per year available for R&D. In addition, the Forensic Laboratory of INS, even though highly regarded, is barely able to purchase the chemicals it needs to function normally, and has no funds at all for R&D.

An area of interest to INS is automated facial recognition. Pattern recognition technology, using video images and sophisticated software algorithms, has progressed to the point where useful and interesting facial recognition equipment may be feasible to develop. The object would be to provide assistance in identifying individuals at ports of entry, when applying for U.S. visas, using photographs or direct observation. In the counterterrorism area, comparison could be made with a file of pictures of known terrorists, because facial measurements preserve a number of known parameters in spite of attempts at disguise and changes due to the aging process.

Although INS has need and use for such work (as do other parts of the Government), it was unable to fund it adequately alone. Therefore, it was forced to seek the assistance of other agencies to find resources to keep such research alive. While INS officials have been somewhat successful in this particular effort, at least up to the present (enabled by informal contacts among scientists working in the field), the haphazard nature of such means of funding is not conducive to an efficient and effective research program. This anecdote, like others previously mentioned, argues for the existence of a better endowed interagency R&D funding group with more effective coordination than now exists.

EXAMPLES OF IMPROVEMENTS IN INTERAGENCY COORDINATION AND COMMUNICATION

Interagency Communications Links

Perhaps the most literal example of lack of effective communication involved the lack of common, secure communications channels among different elements in law enforcement operations (e.g., FBI, Coast Guard, Customs, INS). This deficiency could result in difficulties during combined operations against relatively sophisticated narcotraffickers trying to run contraband into the United States. The efforts of an interagency working group on the topic have resulted in the establishment of secure, common channels that are now available for use.

Redundant Research

In one area of counterterrorism, several highly classified projects were underway in diverse agencies to develop a vital protective tool. There was little communication among the specialists working on the problem, so there was not only a duplication of effort, but also a rate of progress slower than would have been the case if there had been adequate interchange of ideas and information. However, in part due to the forum created by the existence of the TSWG, and in part due to an informal network of contacts among agencies, the problem was identified, and an interagency working group set up in 1990 to coordinate R&D efforts.

As a footnote, an overseas firm and a domestic one are openly marketing a device similar to the one being developed in great secrecy within the government.

Response Plan for Chemical or Biological (CB) Terrorist Attacks

Extensive interagency plans for coordinating a Federal response to nuclear or radiological attacks by terrorists have existed for many years under the leadership of the Department of Energy, with support from the Department of Defense. The implementation of these plans is aided by an array of sophisticated technical equipment. Cooperation among a number of highly specialized response teams from different government agencies has been a principal element in devising these systems.

Until very recently, however, there had been no plan for preparing and coordinating such a response in the case of attack by means of chemical or biological agents, beyond designating the FBI as the response agency and providing for some support by the U.S. Army. This was in spite of assessments by many experts that a CB terrorist attack would be much more likely than a nuclear one.

Fortunately, this deficiency is now being remedied by the development of a response plan involving a large number of agencies, under the leadership of the FBI. Other participating agencies include the Environmental Protection Agency, the Department of Health and Human Services, the Department of Defense, the Department of Agriculture, and the Federal Emergency Management Agency. Appropriate expertise from the most knowledgeable agencies is now being brought to bear on the subjects, and

trained and equipped response forces are being assigned responsibilities in case of such an event. Procedures for rendering assistance to local authorities have been developed. While the plan has not yet been finally implemented, the Nation now has a capability for dealing with this eventuality.

Special Operations Expo '90

In order to stimulate communications among scientists and engineers of the National Laboratories and the military professionals responsible for special operations, the Department of Energy and the U.S. Special Operations Command (SOCOM) of the Department of Defense held a joint exposition in March 1990. Each of the Laboratories working on related technical questions set up exhibits to demonstrate their capabilities to military and technical personnel of SOCOM.[2]

Although this field is not identical to counterterrorism, special operations do include military actions against terrorism, so many of the technologies being researched would apply directly to the topic of this study. Further, other technologies (e.g., sensors) that are useful for low-intensity conflict (the main concern of special operations) would also have applications in the counterterrorist arena.

Many of the participants felt that the exposition was useful in bringing together for the first time technical experts from the laboratories with experts in the operational field. Another such conference was held in November 1991.

Findings and Summary

Direct contact of the above sort between the technical and operational cultures is often an efficient process that cuts through red tape and facilitates transferring information on operational requirements to scientists and information on technological possibilities to the military professionals. This principle could be profitably extended to other fields of counterterrorist endeavor, especially in the relevant areas of the behavioral sciences (in which interagency communication **could be improved, see ch. 5) and in aviation security. Periodic symposia and conferences, bringing together experts from different agencies to exchange ideas and information, are useful and should be increased. There should be an effort to arrange such conferences at least on an annual basis. This might be another function that the TSWG could perform.**

In fact, some such conferences do take place.[3] However, there is a need for more of them sponsored by government agencies in the counterterrorism field, so that technical experts from diverse agencies who rarely communicate with each other could interact. When necessary, they could be held in classified formats.

In summary, there have been a number of recent improvements in interagency coordination. However, there are several areas where coordination of counterterrorist efforts could be upgraded. This applies both to R&D and to technology related to operations.

OPTIONS

In counterterrorism research and development, **two** institutional phenomena are salient. First, in some fields, there is redundancy in research projects. Typically, different agencies spend significant funds, sometimes paying the same vendors, in order to develop similar hardware. Second, some agencies (e.g., INS, the Secret Service, and the FBI), suffering from virtually nonexistent budgets for R&D, yet needing to develop tools for **counterterrorist missions**, are forced to shop around for well-heeled agencies to provide funds to support these efforts.

Both these difficulties should, in principle, be avoided because of the existence of the TSWG and its parent, the Policy Coordinating Committee on Terrorism. These interagency committees are meant to coordinate activities in this area in a way that avoids redundancies and assures that needed work gets done, even if no agency can alone find the funds to perform it. However, as noted in the previous OTA report on technology and terrorism,[4] funding

[2]The DOE Laboratories included were Argonne National Laboratory, Remote Sensing Laboratory/Las Vegas, Idaho National Engineering Laboratory, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, OakRidge National Laboratory, Pacific Northwest Laboratory, Sandia National Laboratory, and the Special Technology Laboratory.

[3]For example, the American Defense Preparedness Association (ADPA) has been organizing annual meetings on security technology fOr 7 years. Also, the Department of Transportation, together with private sector organizations, has presented yearly meetings on transportation security, and the Federal Bureau of Investigation has periodically put together meetings on explosives detection.

[4]U.S. Congress, Office of Technology Assessment, op. cit., footnote 1.

for the TSWG has been problematic, declining by 80 percent in fiscal year 1991 relative to the level at its inception 5 years ago. Shortage of money apparently increases turf protection and discourages communication among the agencies doing the R&D. It also encourages scientists to use their own informal networks of colleagues and friends in other agencies to seek funding for needed projects-funding that should be assured and coordinated through the interagency group for such research. This approach, while practical for the individual, results in a haphazard allocation of resources.

Politically, it will not be easy to put all counterterrorism R&D under one umbrella, and that should not be the goal. Some agencies (in particular, those of the Intelligence Community and the Defense and Energy Departments) would likely not be interested in having those counterterrorism projects specific to their own missions controlled or subsumed by an interagency group. But those projects with interagency applications, and there are many, both ongoing and proposed, should be coordinated by a central entity. This measure is needed to avoid redundancy of effort and to increase contacts and interaction among scientists doing similar work. Otherwise, current inefficiencies and barriers to communication will continue, hurting the national counterterrorist R&D effort.

The coordinating group should have sufficient funds, respect, and, thus power, to run an efficient program. If substantial research funds are not under control of the coordinating group, it will not be taken as a serious player by the member agencies. To improve communication among participating experts, a larger fraction of the Nation's counterterrorism research should be subject to coordination from a single source than is currently the case. Now, the TSWG represents only $2 million out of over ***$70*** million. Even if expanded to $10 million, this fraction would still be only about 15 percent.

Effective interagency coordination would avoid significant redundancies in research projects. However, coordination is also needed beyond the R&D arena. Efficient interagency exchange of information needs to be implemented. On the R&D plane this could be accomplished by holding interagency technical seminars, for example, and on the operational level by establishing, maintaining, and using interagency charnels of communication. Effective coordination should provide databases on technology and databases and alerts on terrorists and their activities. These should be accessible to all agencies with need for the information.

OTA has identified four options for improved coordination among the many agencies that have R&D interests in counterterrorism.

Option **1: Continue with the TSWG and its parent Policy Coordinating Committee on Terrorism as now funded, run through the Department of State, with a large increase in funding, as now planned, mostly originating from Department of Defense funds. Give the TSWG its own line item in the State Department budget.**

Advantages. This continues the present institutional situation, which has worked until now, although hampered by funding constraints. Many of the participants are familiar and comfortable with it. The increase in funding (proposed to $10 million from $2 million), if implemented, should be sufficient to assure that needed projects, particularly of research-starved agencies, are undertaken. This setup allows decisions on research to be made by a committee made up of representatives of all the participating agencies. It is meant to assure that the large research agencies (e.g., Defense and Energy) will not dominate or gobble up the research pie.

A line-item status will help assure that other components of the State Department do not drain funds intended for the TSWG. It may also help in providing an incentive for the State Department to give more active support to the TSWG when appealing for funds from Congress.

Disadvantages. There may remain some congressional opposition to funding a research program through State, which is not a research-oriented agency. The funding may never be assured from year to year, unless strong advocates appear, either in Congress or the executive branch. Power and decisionmaking maybe perceived as tilting towards Defense, since a large share of funds will be supplied from their budget. Defense is already managing the program for State, which has limited technical expertise.

Option 2: Place the TSWG in a major research agency, such as the Department of Defense, the Department of Energy, or the Department of

Transportation (now a major participant in counterterrorism R&D). Give it a line item.

Advantages. The Departments of Defense and Energy both have significant experience in managing R&D programs of all sizes and at all phases. Stable funding would be more likely; even if the congressional allotments were to fluctuate, the host agency could make up differences in lean years, since the whole program would constitute a minute part of the agency's research program.

Disadvantages. There could be distrust among other participating agencies, since the perception will be that the host agency will take the lion's share of projects. A committee may make funding decisions, but the power of the purse of the host agency might swing decisions in favor of research it particularly wants. On the other hand, the host agency may not want the program, since it may perceive that the cost of TSWG research, primarily done **to satisfy** other agencies' needs, would be deducted from its own in-house research.

Option 3: Replace the TSWG with **a** similar funding group **run out of a DOE national laboratory or a smaller agency with research capability. Give it a line item.**

Advantages. A laboratory would be familiar with science and engineering issues and research practices, which would help in furnishing competent oversight. An operational agency would be aware of the field requirements of the equipment. In the former case, the TSWG would be somewhat removed from interagency rivalry, although subject to interlaboratory rivalry.

Disadvantages. This would place much power, probably too much, in the hands of only one participating agency, even if accompanied by an interagency oversight board. Since the TSWG would be replaced, many old players would likely not be enthusiastic, especially State, Defense, and Energy, all of which had leading roles. If the location were a national laboratory, Energy might be somewhat mollified.

Option 4: Replace the TSWG with a similar funding group operating out of a technical office close to the President with no direct interest in doing research itself, such as the President's Office of Science and Technology Policy, or the National Security Council (NSC), or out of a new office, following the model of the Office of National Drug Control Policy.

Advantages. The coordinating body would be in a strong position of power (if actively supported by the White House) and thus able to arbitrate among agencies and deal **with rivalries** and parochial interests. A strong position would also help in eliciting information from reluctant participants and in fighting turf builders. If located in the White House Office of Science and Technology Policy (OSTP), the coordinating group would be likely to have strong technical input. It could also benefit from the perception that the OSTP would be a disinterested, honest broker. This would also apply to the creation of a new office. Also, this option might provide **a** good place to take advantage of existing talent to deal with the multidisciplinary needs of overseeing a highly varied program. A new office would have to receive separate research funding and control the power of the purse strings, otherwise participating agencies would not be interested in playing. This option might level the playing field among agencies in that more weight might be given to the needs of agencies with limited R&D budgets (e.g., Secret Service, INS).

Disadvantages. The TSWG would disappear, thus irritating the same participants as in the previous option. A new arrangement for counterterrorism R&D would exist, making long-time participants uncomfortable. Major agencies might be more reluctant to play. Congress maybe reluctant to fund anew agency or to increase significantly the budget for an existing office. The OSTP or NSC might be reluctant to take on the task of managing research, particularly in a narrow area.

INTERNATIONAL COOPERATION

The United States engages in cooperative efforts in the field of counterterrorism with a number of its allies and in some international forums. The United States works most closely with Canada and the United Kingdom. Collaboration with the Canadians is especially active in the areas of explosives detection and airline security. Several firms with competitive vapor detectors are Canadian; Canadian experts participate with U.S. agencies in discussions regarding research into airline security. Periodic counterterrorism exercises are held with the Canadians.

The United States also exchanges information with the United Kingdom in a number of areas relevant to counterterrorism. One thermal neutron analysis (TNA) machine for explosives detection, developed for the Federal Aviation Administration (FAA), is being tested at Gatwick airport near London, in cooperation with British airport authorities. There are also exchanges of information with other European allies. In all cases, however, there is technical information considered so vital to national security that no party will exchange it with another.

Some research projects in other countries are funded by U.S. agencies. For example, scientists at the Soreq Nuclear Research Center in Israel are, in collaboration with scientists from Los Alamos National Laboratory, working on developing the nuclear resonance absorption technique for explosives detection. The joint effort is funded by the FAA. This project also involves interagency cooperation, since Los Alamos is a National Laboratory of the Department of Energy: an interagency agreement between the FAA and the Department of Energy enabled this collaboration on a national level. The FAA is examining a Soreq bomb detecting device employing advanced x-ray techniques. A Memorandum of Cooperation between the FAA and the Israeli Airports Authority was signed to permit the international effort between FAA and Soreq.

There are efforts to establish research collaborations on other topics between U.S. and foreign scientists, particularly those in Western Europe. Recently, the Soviets have expressed an interest in technical exchanges on counterterrorist technology, probably reflecting a concern with internal ethnic discontent and the large number of hijackings within the past 2 years. Such collaborations and exchanges of information also may have the added advantage of saving money in research efforts.

In addition to formal collaborations at the intergovernmental level, there are periodic international conferences on explosives detection that result in useful exchanges of information.

Regarding international organizations, the International Civil Aviation Organization (ICAO), an agency of the United Nations, has recently concluded a draft **treaty** on tagging explosives during manufactures The United States and Canada, together with France, the United Kingdom, Czechoslovakia, and other European countries were particularly active in bringing this effort to fruition. ICAO is continuing efforts to examine the uses of technology to further international airline security.

Another international effort in which the United States participates is Interpol, the international police organization, which exchanges information on criminals. U.S. officials are assigned to Interpol work, both in the United States and at Interpol's headquarters in Lyons, France. Information on terrorists that is not classified is sent to Interpol by the appropriate U.S. agencies. The United States also receives such information for use when domestic action is feasible. Interpol has recently improved its communications capability and can now send specific pieces of information through secure channels to only those nations authorized to receive it.

The United States also has observer status with the TREVI group, an organization of Western European Interior Ministries, that is concerned with, among other things, exchanging vital information on terrorist activities in Europe.

Contacts between the United States and friendly states in the field of counterterrorist technologies could usefully be expanded. In particular, security practices at airports in Switzerland and Israel are, in many aspects, more advanced than those in the United States. U.S. agencies have, in fact, participated in discussions with officials of both countries, but more exchange of information would be advantageous. Moreover, researchers in other countries, notably Israel, Canada, Australia, and the United Kingdom, have made some technical advances that could be of use to the United States. Much U.S. technology could be made available to friendly states without compromising national security interests.

[5]See U.S. Congress, Office of Technology Assessment, op. cit., footnote 1, pp. 50-51.

Chapter 4

Aviation Security: Aspects of Integrated Security for Commercial Air Travel

Contents

Figures

Chapter 4

Aviation Security: Aspects of Integrated Security for Commercial Air Travel

INTRODUCTION

Over the last 10 years, high-capacity international aircraft have become favorite targets of terrorists. Consequently, much research and development in counterterrorist technology has been focused on means of safeguarding this mode of transportation, in part by developing better means of detecting the small quantities of explosives believed to have caused the most recent fatal tragedies. That effort has included some attention to controlling access to the aircraft and other critical areas at airports, and to the human aspects of the security system. However, to date, the question of how best to combine technologies and people to provide maximum security is very much open.

Although most past research has looked at each concept or device as a stand-alone answer to the total problem of explosive detection, it is now generally recognized that no single detector either exists or will likely exist in the near future that can provide practical, reliable detection of explosives of the types and quantities of concern to aviation security. Recent reports by the National Academy of Sciences (NAS),[1] as well as by the Office of Technology Assessment (OTA),[2] concluded that a combination of techniques and devices is the most promising means of attaining high-confidence protection from explosive devices.

To determine how such a combination may reasonably be achieved, the performance of current and near-term technologies must be analyzed. Further, it is necessary to consider how various technologies and techniques best complement each other.

INTEGRATED SECURITY SYSTEMS

A systems approach to overall airport security is under development in a major program sponsored by the FAA Technical Center, using the Baltimore/Washington International Airport (BWI) as a model. The development is being supported by Sandia National Laboratories, under contract to the FAA Technical Center.[3] This program is attempting to find the proper balance among risk, technology, and operational considerations for a typical airport environment, using BWI as a typical airport model. The program also will attempt to generalize the results found at BWI to other airports, by means of computer modeling. This program considers all the fictions of a security system, from detection to delaying intruders and response to intrusion.

COMBINED TECHNOLOGIES FOR AN EXPLOSIVES DETECTION SYSTEM

The explosives detection problem is one of surveying all means of bringing explosives aboard aircraft. First, this means screening passengers as well as hand-carried baggage and checked baggage that go on board. Mail and cargo must also be considered as possible pathways for introducing explosives aboard aircraft. Screening all flightcrew and service and airport contractor personnel is yet another issue, covered by the BWI program but not considered here.

---

[1] National Academy of Science, Committee on Commercial Aviation Security, National Materials Advisory Board, "Summary: Reducing the Risk of Explosives on Commercial Aircraft," NMAB-463, 1990.

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

[3] The FAA BWI program is a multiyear systems study of security at the airport. The project began with an analysis of the airport/aircraft access problem, utilizing computer modeling and (human) expert input, new procedures, and training. It will follow with implementation, using these inputs and also encompassing hardware at the BWI airport at one of the domestic piers and the surrounding aircraft operations area.

Some general concepts must be considered in quantifying the explosives detection problem. These include the statistical parameters generally used to define the performance of detection devices, the statistics used to describe systems composed of combinations of detectors, the flow rate through the baggage checking system, and the throughput of a single device.

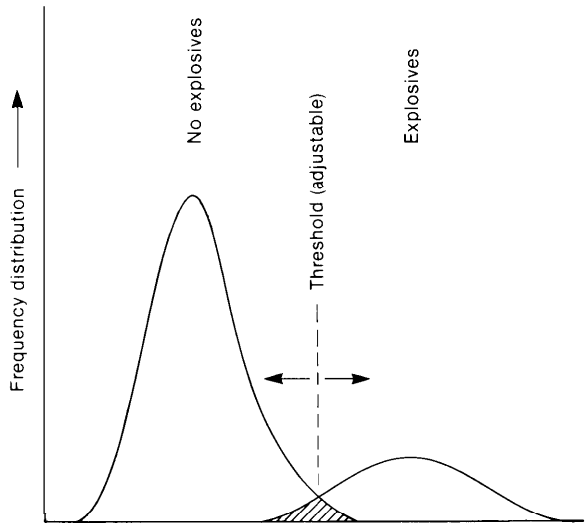
Statistics of Detection

The performance of a detection system can be characterized by two primary parameters: the detection probability, P_d, and the false alarm or false positive rate, F_a. A good detector has a very high detection probability (as close to 100 percent as possible), while still maintaining a very low rate of false positives or false alarms. These two parameters are coupled, primarily through the detection threshold: the more sensitive the detection threshold, the higher the false alarm rate. Unfortunately, to detect small quantities of explosives with high probability requires that the threshold for detection (the lower limit on the amount of explosives that may be reliably detected) be set as low as possible; consequently, the false alarm rate is high. This effect is shown graphically in figure 4-1. The curve on the left represents the distribution of measured nitrogen content (or other detection parameter) for bags with no explosives. The curve on the right represents the distribution of measured nitrogen content for bags with a given amount of explosives that should be detected. The shaded area of overlap represents the probability of a signal being caused by either a clean piece mistakenly identified or by a piece of contraband material.

As the threshold is moved to the left, i.e., the device is adjusted to detect lesser quantities of explosives, the detection probability for explosives increases (i.e., a greater percentage Of the total explosives population is correctly identified) but a larger area of the signals from clean items is included in the uncertain population, representing a higher false alarm rate.

Any detection scheme depends on a separation of the two peaks: the probability distribution of the clean items and that of the explosive. Figure 4-1 also demonstrates that as the quantity of explosive to be detected decreases, the two curves move together (i.e., the distribution of signals from bags with explosives will be shifted to the left), making discrimination more difficult.

Figure 4-l—Generic Frequency Distributions of Detections and False Alarms



SOURCE: Office of Technology Assessment, 1991.

One way of increasing the effectiveness of a detection system is to combine several diverse detection techniques that make use of different phenomena. When two *independent* measurements are *both* required in order to produce an alarm (an "AND" gate) in a single detection system, the combined effectiveness in terms of overall detection probability, P_{dc}, is the product of the two individual probabilities, or $P_{dc} = p_{d1} * p_{d2}$, and the false alarm rate, F_{ac}, is the product of the two individual rates, $F_{ac} = F_{a1} * F_{a2}$. The combined probability, P_{dc}, is always smaller than the individual ones. Since detection with a high probability is the name of the game (P_d on the order of 0.90 or better is usually set as the goal), all stages of a system must individually have high detection probability. Combining two poor detectors thus does not necessarily make a better system in terms of detection probability. It is also possible to combine two detectors so that an alarm from *either* one may trigger remedial action or examination by yet another device (an "OR" gate). In this case, the resulting detection probability (and false alarm rate) combine as $P_{dc} = P_{d1} + (1 - P_{a1}) * P_{d2}$. The detection probability will increase relative

to that of the individual detector, but so will the false alarm rate.

Significant gains can be made in the area of false alarm reduction by combining several detectors, each with moderate performance in the false alarm area. Two detectors each with an unacceptably high false alarm rate of, say, 20 percent would combine in an "AND' logic to produce a false alarm rate of only 4 percent, if the two measurements were truly independent. (In fact, they often will not be totally independent, so these arguments apply only to an idealized case. However, for some combinations of detectors (e.g., vapor detectors and TNA), the phenomena used are totally distinct, approximating the ideal.) A strategy of multidetector systems can be based on the goal of achieving an acceptable false alarm rate (often 5 percent or less) with acceptable detection probability. Depending on the parameters of the component devices, this may require AND gates, OR gates, or some combination of the two.

The true combined detection probabilities and false alarm rates can only be determined by measurements in an operational environment. Because of real interferants (e.g., objects that really contain large amounts of nitrogen and are dense), the combined probabilities will never be as good as the theoretical ideal. The above statistical arguments only provide an indication of possible improvements in combining systems, not a precise theoretical prediction of operational results.[4]

Detection Criteria

What actually constitutes acceptable detection probability and false alarm rate is not easily determined. The former is a question of acceptable risk while the latter is an operational problem. Setting the minimum acceptable detection probability is a subjective issue. If there were 10 attempted bombings per year (out of 40 million international enplanements), a detection probability of 0.90 would allow one expected dangerous situation (and sometimes more) to go undetected per year. If there were only one bomb attempt per year, the statistical expectation would be for one to go undetected about every 10 years. Would a terrorist be deterred by these odds and would the flying public accept them as "safe"? The operational part of the problem can be analyzed reasonably objectively, yet it, too, is difficult to specify precisely.

Flow Rate or Throughput

The Air Transport Association (ATA) contracted with the Institute of Transportation Studies of the University of California at Berkeley[5] to perform an analysis of the operational problems of installing a TNA-based explosives detection system (EDS) as specified by the FAA.[6] This study focused primarily, but not exclusively, on a false alarm rate of about 5 percent, as specified by the FAA for an EDS. Among other findings, the study found that the throughput of the Xenis (TNA plus x-ray)[7] EDS had to be slowed down by 28 percent for automatic detection (from an already degraded throughput of 6 to 7 bags per minute, due to the mechanics of preventing a radiation hazard) to allow the TNA image to be maintained long enough so that it can be correlated automatically with the Xenis X-Ray image. (This is a real effect but not necessarily a permanent problem, since a storage buffer could be added to the TNA computer to maintain the image data from one object while a new object is being viewed.) The study also found that attention must be paid to the space requirement for rejected luggage for any false alarm rate, whether the alarming bags are recycled, sent to another detector, or hand searched. For a 300-bag-per-hour throughput rate, a 5-percent false alarm rate requires space for handling another 15 bags per hour. This could be a serious consideration at the much higher false alarm rates currently encountered by the Xenis EDS. Such operational issues make it difficult to set a generally applicable criterion for the throughput performance requirements of detection systems.

[4]The FAA Technical Center is planning to institute a program called X-TRIALS, which will put a variety of detection devices (covering passengers, cargo, and other potential pathways for the introduction of explosives aboard aircraft) and other elements of an integrated security system in operating airport environments. Such operational experiments are the best way to assess the capability of the elements of a security system and the combined efficacy of parts of the system at the same time.

[5]Geoffrey D. Goslin and Mark M. Hansen, "Practicability of screening International Checked Baggage for U.S. Airlines," Institute of Transportation Studies, University of California at Berkeley, Research Report UCB-ITS-RR-90-14, July 1990.

[6]See 54 *Federal Register* 36938, (Sept. 5, 1989).

[7]The systems tested at Gatwick and Kennedy Airports combine a TNA device with an x-ray systems to compare and correlate information 011 excess nitrogen density with information onhigher density objects in the bag.

The analytical model developed in the Berkeley report has some capability for investigating the impact of higher false alarm rates on the operational difficulties of the airlines and consequently could be used to set objective guidelines for the maximum acceptable false alarm rate in a given operational situation.

The FAA, both in its research and development program and in its rule making process, has arbitrarily settled on a handling rate of 600 bags per hour (or 10 per minute). Realistically, however, the throughput requirement should vary greatly, depending on where in a chain of detectors a specific instrument is being used (and where the device is located). For instance, a device used only on a small number of bags could take much more time for its inspection. If only 10 to 15 percent of the passengers were selected for detailed inspection as a result of a well-defined profiling system, the throughput of the subsequent detection system would be greatly relieved. Further, location of the instrument and detector cost also greatly influence the throughput requirement. Inexpensive systems placed at the check-in counter could certainly allow as much as 30 seconds per passenger since the check-in process takes at least that much time. The issue of throughput requirement may be left to the marketplace, where different instruments with different throughput rates could be combined by the individual purchaser.

In this context, the variability of international airports and gateways should also be emphasized. U.S.-flag international air carriers enplane international passengers at 190 different airports, the top 20 of which carry 52 percent of the 38 million enplanements (19.5 million). The largest five airports handle an average of 1.8 million passengers per year and the other 15 of the top 20 carry only an average of 700,000 passengers per year. The other 170 airports handle considerably fewer passengers, on the average only about 100,000 per year. Thus, the high-volume gateways are an exception, rather than the rule, and much of the equipment required for a national security system will need to handle only moderate rates of baggage throughput. The detection system criterion for throughput will vary greatly; the choice for any specific operation **may best be left to the users, based on operational considerations.**

RECENT DEVELOPMENTS IN DETECTION TECHNOLOGY

X-ray Systems for Bomb Detection in Baggage

X-ray technologies for airport security are developing rapidly as advanced systems used for medical and industrial imaging are adapted for screening luggage. The FAA tested some advanced commercial x-ray systems in late 1990 for specific purposes in baggage screening. The results of these tests have not yet been released.

The standard x-ray machine for airport security produces an image of the distribution of x rays that have passed through the observed object. These pictures have excellent spatial resolution-thin wires are readily seen—but the operator cannot find a lightweight object behind a denser one, nor tell whether a dark image is due to a thin sheet of a heavy material, such as steel, or a thick sheet of plastic, which can produce the same x-ray absorption. During the past few years, a number of companies, using a variety of approaches, have been trying to overcome these shortcomings.

Dual-Energy

Dual-energy x-ray inspection produces two images, each taken with a different range of x-ray energies. Comparing the images yields information on the average atomic number of the elements in the material traversed by the beam.[8] Such machines can distinguish between metals (e.g., steel) and plastics. As yet, however, no commercial machine of this type can distinguish between some plastics and explosives or books. Moreover, none can detect a lighter object behind a heavier one. This latter problem is being addressed by applying image processing and by employing multiple-view systems.

Image-Processed Dual-Energy

Dual-energy combined with automated image subtraction is being developed by several x-ray companies. The images, stored as an array of

[8]The atomic number of an element is the number of protons (or, equivalently, the number of electrons) in an atom. Atomic weight is proportional to the number of protons and neutrons in an atomic nucleus. For light elements, the atomic number is roughly proportional to atomic weight; for heavier elements, atomic number increases at a slightly lower rate than atomic weight.

numbers, are manipulated by sophisticated computer algorithms that try to identify and isolate objects from their backgrounds. The dual-energy method is then applied to the isolated objects and an alarm produced if the characteristics of the object match those of a presumed explosive. Although a clear technical advance over simple dual-energy, it remains to be proven how well such a technique will work in a real airport environment.

Vivid Technologies of Waltham, MA, starting from expertise developed in producing special purpose medical x-ray equipment, has produced a refined dual-energy, single-view x-ray machine that can, it is claimed, very precisely determine the effective atomic weight and x-ray absorption density of all items in a piece of luggage. It does this by comparing high-resolution images at two x-ray energies and then using advanced computing techniques to analyze the images. Explosives of interest are claimed to give a definite signature of well-defined effective atomic numbers and densities.

Dual-Axis, Dual-Energy

EG&G Astrophysics, of Long Beach, CA, under contract with the FAA, is developing a dual-energy, dual-view system (T-Scan™—a trademark) that may determine effective atomic numbers by comparing views at different energies. EG&G uses two perpendicular views, rather than highly sophisticated computing algorithms, to resolve confusion in the images due to overlap of objects. The system is intended to have the ability to determine average atomic numbers along the perpendicular directions of view.

X-ray Compton Scattering

American Science and Engineering (AS&E) obtains backward x-ray scattering and x-ray transmission images simultaneously. A comparison of the two images gives the atomic number of interior objects with definition comparable to that from dual-energy techniques.[9] It has the advantage in some cases, such as bombs hidden in baggage linings, of being more sensitive than other techniques. However, the backward scattered image is made by lower energy x rays that are more easily absorbed by heavy material. AS&E is also developing image processing techniques and employing different scattering strategies to improve detection capabilities and is working on an automated algorithm to alarm in the presence of explosives.

Multi-Energy Imaging

Instead of imaging at two energies, it is possible to image many energies at the same time. One company, Magal of Israel, is marketing an instrument that manipulates the information generated with pattern-recognition algorithms. A great deal of additional information is thus available for analysis. The device is purported to give automatic alarms in the presence of bomb components.

Computerized X-ray Tomography

During the past year there has been a series of FM-sponsored tests at Imatron Corp., to evaluate the current performance of an x-ray computerized tomography (CT) scanner under development there. Whereas the original development at Imatron had aimed at a stand-alone EDS system, these tests emphasized its compatibility in combination with the SAIC/TNA. A group of bags that had alarmed the TNA system were delivered to Imatron with the location of the suspected area marked on the outside of each bag. Some of them actually contained real explosives (PETN and SEMTEX). Since the TNA has only moderate spatial resolution, the marking essentially consisted only of information on which quadrant of the bag contained the suspected explosives. The Imatron CT then looked only at the suspect area by making 3 to 10 CT slices of this area to produce reconstructed images (a l-cm thick segment of the object is imaged in each slice).

The results from this series of tests, although preliminary due to the small sample size and ad hoc nature of the tests, were quite encouraging.

The current Imatron CT seamer has a 60-cm-diameter detector ring and is not large enough to handle many common pieces of luggage. A new model with an 80-cm-diameter ring, which can handle baggage equal in size to that handled by the current SAIC/TNA, is currently under construction (under FAA contract). The biggest problem of the system is its scan speed, which is currently about 6 seconds per slice. It is claimed by the vendor, that, in the future, this scan time will be reduced to only 2 to 3 seconds in the new system. The primary issue to be resolved is the number of slices required to provide the needed detection probability (i.e., the

[9] See U.S. Congress, Office of Technology Assessment op. cit., footnote 2, pp. 78-79.

required resolution upon reconstruction). Another important issue is the eventual false alarm rate under operational conditions at an airport. At present, it cannot be ascertained whether the total detection time will be on the order of 10 seconds or a minute or more.

However, any scan time in the above range could find significant applications if the CT scanner were incorporated properly into a total detection system. With a l-minute total detection time, the CT seamer could still resolve false alarms for a system running at TNA speeds having a false alarm rate of almost 20 percent. If the time requirement were relaxed, the system could handle larger first-pass false alarm rates, greater baggage throughput, or could be used at an earlier stage of the detection cascade.

Imatron has also been developing a dual-energy CT detector. A prototype has been built and tested. It is slow, but could be used for close inspection of areas of luggage flagged by other means of screening.

Coherent X-Ray Radiography

Solid explosives are crystalline materials. Each type-PETN, RDX, dynamite, etc.—has a unique crystal structure that is different from that of other explosives and of innocuous materials. The distance between layers of atoms in the structure is revealed by using x rays in a method called Bragg scattering, after its discoverer. If the distance between the planes of atoms in a particular crystal is d, then Bragg scattering will be at a maximum (i.e., will have a peak in intensity) when x rays of energy E are scattered through an angle w, given by

$$\sin w = k/(Ed)$$

where k is a constant. Alternatively, one can send a broad energy spectrum of x rays through an object and observe the scattered x rays at a fried angle w. Bragg peaks corresponding to crystalline spacings are then looked for in the scattered energy spectrum. The method looks for the characteristic spacing of crystals of explosives that may constitute a bomb. The question to resolve is how often other crystals found in luggage or in other examined objects may have a similar characteristic spacing, resulting in false alarms. Scientists at Philips Gmbh of Hamburg, Germany, are developing the method for medical applications and have licensed Scan-Tech of New Jersey for applications in the area of security.

Scan-Tech, in collaboration with scientists at Rutgers University, has successfully completed proof-of-principle tests. These early results give some hope that coherent x-ray scattering may become useful for airline and other security applications. The next stage is to build a prototype and test it under realistic airport conditions.

Evaluation of all these new developments, both for detection probability and false alarm rates, awaits rigorous testing by outside parties.[10]

The Use of Pattern Recognition in X-Ray Images

Automated pattern recognition schemes to enhance the ability of x-ray systems to locate threat items such as guns, knives, and electronic components are under development. Such systems are not only automation schemes but are also ways to overcome the human fatigue problem ever present in a repetitive procedure such as x-ray image inspection.

One company in Canada, Array Systems Computing, Inc., has developed (under contract with Transport Canada) a neural-network based system for detecting guns, knives, and hand grenades and is in the process of extending the technique to detecting electronic components. That system uses a dedicated computer that can be added to a standard high-resolution x-ray system. In tests conducted by the company, their system was able to detect guns with over 95-percent detection probability and about a 10-percent false alarm rate. Separate, independent tests conducted by Transport Canada have confirmed these results. The use of such techniques as an operator assist, allowing the operator to concentrate only on high-threat items that alarm the automatic system, appears to be a productive approach to an important aspect of a security system.

Use of such procedures to identify bomb components is also under development. The critical questions are the eventual performance of the system and the difficulty of disguising or hiding such components from such a system. Until the technology is perfected and tested under controlled conditions, it is too early to evaluate the potential of this technique.

[10]The previous OTA study on technology and terrorism recommended that a testing agency outside the FAA should be empowered to assess explosives detectors for efficacy. See U.S. Congress, Office of Technology Assessment op. cit., footnote 2, pp. 8-10.

Early developmental work on such a technique is under way. The goal is to provide x-ray vendors with a plug-in computer card with sufficient capacity and speed that would perform the analysis of the image and make the decision. If such a system can be developed to have a high-detection probability, even with moderate false alarm rates, it may represent a very powerful add-on which could make an ordinary x-ray detection system semi-automatic.

Microdose X-Ray Images for Examining People

A new x-ray approach has been developed that uses extremely small doses of radiation to examine people to find if they are concealing weapons, explosives, or other contraband under their clothes. American Science and Engineering of Cambridge, MA, has adapted its x-ray backscatter technique to this end. A similar approach was developed by AGS Corp. of Hammond, IN, later acquired by IRT of San Diego, CA. The images produced by both techniques are quite clear, indicating a potential effectiveness, but immediately raising legal issues of privacy. Radiation doses are equivalent to a few minutes of natural radiation exposure, and much less than the increased level of exposure to radiation suffered on a flight. Although these are insignificant levels, there would likely be strong public resistance to the mandated use of x rays for airport security. However, this technique would protect against a principal route for bringing explosives aboard aircraft.

New *Results With TNA*

Further FAA testing of a TNA system at Gatwick Airport near London has been reported to show an improvement over its earlier performance.[11] Whereas earlier tests on goal quantities of explosives showed detection probabilities somewhat lower than desirable, the most recent tests were reported to show higher detection probabilities for quantities in the high range of estimates for the size of the Lockerbie bomb. More importantly, the false alarm rate for similar quantities was also reported to have been cut substantially. These results were said to have been obtained mainly through the development of improved detection algorithms and by the education that the neural network system has gained in observing large numbers of real passenger baggage items. However, even the improved false alarm rate is too high to allow use of the TNA device by itself as the only bomb detection mechanism. The TNA system will have to be combined with profiling (as at Gatwick) and, probably, with other technologies. Further, it may be necessary, pending a new assessment of the desired goal quantity of explosive to be detected, to reduce detection thresholds still further. This would require further improvements in the system to keep the false alarm rate to manageable proportions.

The newer results are in the process of being verified by outside consultants, and a final assessment of the capability of TNA awaits confirmation.

If TNA devices are inherently limited by false alarm rates, as some skeptics claim, one possible application could be to use the device only for close examination of individual items selected by other screening methods (e.g., x rays). As an example, if a screening device finds a suspect electronic device in a bag or carry-on item, a TNA device could be used just to inspect it for explosives content. Since electronics equipment would have a low nitrogen fraction, and the mass of the equipment would be less than that of large bags, confusing background would be reduced and the false alarm rate would be much lower.[12]

New *Results With Vapor Detectors*

Several vapor detectors were tested by the FAA in late 1990 for specific applications in screening luggage. The results of these tests have not yet been made available.

Electromagnetic Techniques for Explosives Detection

A detailed discussion of nuclear magnetic resonance (NMR) and nuclear quadruple resonance (NQR) techniques for detecting explosive compounds is given in CLASSIFIED appendix F. Both methods involve applying radiofrequency radiation to an examined object while observing the electromagnetic response of molecules contained therein. Another method, dielectrometry, measures the dielectric constant (a physical property of matter) of an object, to determine whether anomalous items are

[11] Lynne Osmus, Office of Civil Aviation Security, FAA, testimony at hearings before the Senate Governmental Affairs Committee, Feb. 26, 1991, and Ken Lauterstein, FAA, personal communication, Feb. 1991.

[12] This *suggestion* was made by John Baldeschwieler, Professor of Chemistry, California Institute of Technology, and Chair of the National Academy of Sciences Committee on Commercial Aviation Security, personal communication, July, 1991.

present. The latter technique does not detect explosives, just anomalies in dielectric constant. All these methods can, in principle, be defeated by wrapping the explosive in metal foil. However, it is easy to test for the presence of metal foil, for example, with standard metal detectors (see app. C). For carry-on baggage, there would be a high false alarm rate. However, for screening individual items targeted by other techniques, these methods might be useful. For screening people, NQR might become a candidate detector.

The relative values (among themselves) of NMR, NQR, and dielectrometry depends on the details of the particular application: on the explosives compound, on the nature of the objects that would be used to conceal the explosives, and on the acceptable trade-off between the probability of detection and the false alarm rate. But there are generic differences among the three techniques.

Dielectrometry is the cheapest and most portable option, and it can be very sensitive. However, the response is nonspecific: not only is there little ability to discriminate, but the false alarm rate will be high, as many materials will appear to be anomalies. Nevertheless, in some applications, such as items concealed on a person, the technique maybe useful.

NQR has high specificity, and therefore might produce the lowest false alarm rate. However, the technique may be limited in the number of explosives reliably detectable. One developer has estimated that aversion might cost about $50,000, much more than a dielectrometer, but half as much (or less) as an NMR device. In combination with a metal detector, NQR might be a very useful technique for frisking people for contraband explosives (and could be used for drugs as well).

For baggage inspection, NMR would probably not be as specific as NQR, but it might be effective for a greater number of explosive species. NMR would require the imposition of a strong magnetic field on the baggage, presenting other operational problems (data on magnetic disks carried in baggage would be destroyed, etc.).

Throughputs for all three techniques might eventually be as high as a few seconds per bag.

Associated Particle Production

This technique has been looked at for a number of years, and some researchers have received FAA funding to examine its feasibility for a number of applications.[13] It utilizes a nuclear reaction between two kinds of hydrogen that produces helium nuclei and neutrons at a well-defined energy. Characteristic garoma rays are produced by each element when neutrons strike their nuclei. It is, in principle, possible to measure the relative amounts and locations of nitrogen, carbon, and oxygen in a sample using this method. This technique would greatly reduce false alarm rates because all important elements that constitute explosives could be measured.

However, problems with this approach in the past have included limited accelerator tube lifetimes and slow measurement times. If the reaction is made more intense to produce more neutrons, the tube tends to burnout earlier and a requirement for a large amount of unwieldy shielding is generated.

Nuclear Diagnostic Systems, Inc., of Springfield, VA, asserts that it can produce a useful system based on this technique within a few months. The company claims that it has a tube that lasts sufficiently long to be practical for a number of applications, including airport security, and that needs to function at such a low level of neutron production that no shielding would be required. The researchers have received support from private sources for this development. Again, testing by outside parties will be needed for a proper evaluation of the claims.

PASSENGER/BAGGAGE MATCHING

In June 1985, an Air India flight enroute from Montreal to London was destroyed by an explosion over the North Atlantic; Sikh terrorists claimed responsibility. Investigators believe that an unaccompanied checked piece of luggage contained the bomb that caused the explosion. Since most terrorists are not suicidal (despite press attention to the contrary),[14] ensuring that all checked luggage belongs to passengers who have actually enplaned is an effective frost line of defense against this threat.

[13] U.S. Congress, Office of Technology Assessment, op. cit., footnote 2, pp. 74-75.

[14] Thomas Strentz, FBI/FAA profiling contractor, personal communication, NOV. 9, 1990.

Effective December 1990, the FAA required all U.S. carriers to ensure that all personal baggage carried on international flights of U.S. airlines be positively matched to passengers who board the flight. Unaccompanied baggage can be transported only after "close scrutiny. "[15] These FAA requirements are similar to current International Civil Aviation Organization guidelines. FAA does not mandate a specific technology to accomplish this task; airlines are free to choose the approach that suits their traffic levels and organizational structure.

Most airlines use a manual approach, especially where traffic levels are low, by inspecting each passenger's baggage claim tickets at the aircraft gate and coordinating the loading of the corresponding bags. For example, American Airlines baggage tags have peel-off sections that the baggage handlers attach to the cargo containers when the bags are loaded; a telephone or radio link is maintained between the gate and the loading area and the handlers annotate the corresponding tags and a master list as the passengers board the aircraft.[16] Some airlines are testing bar-code-reading equipment to speed the matching process and are using information systems to track where each bag is placed, permitting quick baggage retrieval when necessary. On aircraft that are not wide-bodied, such as the Boeing 727, baggage cannot easily be containerized, making the retrieval process more time consuming. Northwest Airlines has installed bar-code-reading and data-communication equipment at all stations, and uses it for all international (and some domestic) flights.[17] Trans World Airlines has also begun applying bar-code technology.

For domestic travel, airlines cite the volume of traffic and the use of smaller aircraft as reasons making passenger/baggage matching difficult (without enormous delays and drastically altered current flight schedules). However, in the domestic case, it would be possible at least to apply matching on a limited basis: using profiling information to select a subset of passengers and bags for close scrutiny, or giving priority to matching interline baggage, **for example.**

In spite of these disparate efforts, there has been no standard defined nor has there been a demonstration of generally available equipment that makes this process operationally practical. A key problem is the difficulty of interline and intraline baggage checking. Further, it is essential to check that baggage introduced as interline transfers be matched to an enplaned passenger or subject to careful examination.[18] The transfer of baggage between connecting flights at the points of departure to or from the United States must be controlled, whether the same or a different airline is used. This is a much more formidable problem for outbound international flights because of the U.S. system of airline hub cities. A simple solution would be not to allow through checking, but this would be unacceptable to the airlines and, probably, to the flying public. Straight-through checking is very important to U.S. airlines as a major selling point. One solution to the problem of controlling baggage checked through to international destinations presents airlines with the difficulty of checking baggage to international standards at additional airports that by themselves do not handle any international traffic. Current practice for most airlines appears to be the use of modern x-ray equipment at the first check-in point. This is not currently a very good detection scheme for explosives.

However, it appears that all the technological elements of an effective automated (or at least semi-automatic) positive baggage matching system are available. For instance, one might use bar codes or magnetic tape, scanners, and dedicated local area computer networks. Bar codes on the baggage tag as well as on the passenger ticket already identify all baggage in some airlines. These bar codes on the baggage could also track the baggage from the check-in counter to the aircraft. The attendant checking tickets at the airplane gate could scan the code while taking the ticket, thereby releasing that bag to be placed on the aircraft. The scanner would be networked to a terminal on the apron that relays the information to the baggage handlers. Each baggage container could have a manifest, listing each bag in the container (either with bar codes or in

[15] Close scrutiny'' is language from the guidelines developed by the International Civil Aviation Organization. Lynne Osmus, Office Of Aviation Security, FAA, personal communication, Feb. 22, 1991.

[16] Homer Boynton, Chief of Security, American Airlines, personal communication and site visit, Dec. 3, 1990.

[17] Douglas R. r&d, Director of Security, Northwest Airlines, personal communication, Feb. 22, 1991.

[18] It appears that the luggage containing the bomb that destroyed Pan Am 103 was introduced as **interline baggage at** Frankfurt.

the apron computer terminal) and baggage could be held out from loading until the passengers owning the listed baggage had boarded.[19] A key operational problem is how to handle the bags awaiting the passenger's arrival. Since aircraft are commonly loaded by seat numbers, it has been suggested that the baggage could be loaded into containers in similar order. Missing or last-minute passengers could present problems, and some containers may have to be held out until the last passenger shows. Another alternative would be to load passengers by paging, with the roster correlated to containers. All these procedures could be foiled by last-minute arrivals, but these passengers do not usually have their checked baggage placed in containers anyway. Interline passengers, often late, also sometimes fall into this category. If the bar-code systems are made sufficiently uniform between airlines, application of these techniques could solve the interline baggage problem.

Finally, positive matching of baggage with passengers is useful only insofar as the baggage handlers are trustworthy. If suborned, they could subvert any mechanical system. As in many other aspects of security, the human element is essential (see further discussion on background checks for airline and airport employees under section on access control, below).

Research and Development

A few years ago, FAA considered conducting R&D for passenger/baggage matching technologies, but the airline industry position was that the airlines could handle it themselves (and they did). However, the FAA Aviation Security Research and Development Service has recently issued a contract for ongoing R&D to develop further refinements of the technology for future systems.

AIRCRAFT HARDENING

The difficulty of developing explosives detectors for currently accepted minimum threat levels for aircraft has focused new attention on the possibility of hardening either the aircraft or the baggage containers so that they could withstand a threat substantially in excess of this minimum. Both the President's Commission on Aviation Security and Terrorism[20] and the study of the Committee on Commercial Aviation Security of the National Academy of Science[21] recommended serious efforts to evaluate the potential of this approach. Success at such an effort could greatly simplify the detection problem. Of the two, aircraft or container hardening, the latter seems to be a more feasible approach since any change to the aircraft structure would require significant airworthiness recertification efforts and costs.

The susceptibility of modern aircraft to fatal damage by explosives has been under study at the FAA for some time. However, this effort has so far been primarily an empirical approach. In particular, aircraft have been tested by exploding various quantities of explosives in diverse locations to attempt to determine a least-damage location on board the aircraft, as well as to find the minimum quantity of explosive that could cause catastrophic damage in flight. Unfortunately, such tests are usually nonflying, static tests and they involve many variables (location of bomb, types of surrounding baggage, etc.). Exploring the effects of all these variables would take an inordinate amount of tests and would thus be impractical.

In 1990, the FAA Technical Center conducted a 3-day meeting to discuss and plan a new program to evaluate the potential of these techniques. The result of this meeting has been the development of a multiyear plan of attack on the problem of aircraft hardening to resist in-flight explosions.[22] The report has been submitted to the administrator for approval. A key ingredient of this new program is a strong analytical effort to adapt and apply currently existing computer codes, both for the effect of the explosion (e.g., several DOD-developed codes or DOE's LASNIX) and for the structural response (e.g., NASA's NASTRAN) to the problem. Use of such numerical simulation is a vital addition to the

[19] Some airlines, notably Northwest and Trans World, are now implementing such systems.

[20] The White House, Report *of the President's Commission on Aviation Security and Terrorism, (Washington* DC: The White House, May 15, 1990), p. 66, recommendation 5: "The FAA should conduct research to develop the means of minimizing airframe damage that may be caused by small amounts of explosives."

[21] National Academy of Sciences, Committee on Commercial Aviation Security, op. cit., footnote 1, pp. 3-5.

[22] Department of Transportation, Federal Aviation Administration Technical Center, *Aviation Security* Research *and Development Plan for Aircraft Hardening* (Washington, DC: Federal Aviation Administration, August 1990).

FAA program. Such codes, combined with carefully designed calibration tests to anchor them to reality, will be of use in defining the problem and synthesizing possible countermeasures.

The last line of defense against an airline terrorist is the aircraft itself. Although the design and operating environment of a passenger airliner (lightweight structure, sensitive controls, pressurized fuselage) make it very vulnerable to internal detonations, there are potential ways to limit explosive damage. Possibilities include the containing, controlled venting, or the absorption of explosive shock waves and gas pressures. By raising the minimum quantity of explosives needed to destroy an aircraft, hardening could complement airport-based passenger and baggage screening technologies, since the detection probability of all devices increases with the amount of target explosive, and the concomitant use of higher detection thresholds would also reduce the false alarm rate.

The British Department of Transport, following its investigation of the Lockerbie incident, recommended that government authorities, aircraft manufacturers, and other interested parties "undertake a systematic study with a view to identifying measures that might mitigate the effects of explosive devices and improve the tolerance of aircraft structure and systems to explosive damage. ' '[23]

This report was able to rely on an unusually complete analysis, because the accident occurred over land and a large fraction of all the parts involved in the explosion were recovered and reconstructed. The investigation found that there were at least three separate effects that contributed to the loss of the aircraft. First, the direct or blast damage, resulting in a relatively small hole (the shattered region was only 45 to 50 centimeters) through the skin of the fuselage; second, the propagation of cracks emanating from this jagged hole to distances as large as 12 meters, which were driven both by the blast pressure and by the aerodynamic forces on the peeled back skin; and finally, further skin ruptures, driven by overpressure from the blast and from gas dynamic shock propagation through open passages between the skin and the baggage containers (and other ducts), which occurred at large distances away from the hole. These latter shock waves finally met obstructions that created local areas of high overpressure due to shock reflections. According to the British analysis, it was the combined phenomena of these forces that led to the disintegration of the aircraft. Other investigators, however, remain skeptical as to the importance of distant shock wave propagation within the fuselage and feel that static pressure was the principal cause of the catastrophic failure. The issue may be resolvable by further testing. The British report indicated that the failure was a complex process and was specific to the local geometry.

Explosive devices of the size used in airline terrorist events to date are deadly not because they directly cause catastrophic failure (i.e., blow the aircraft to pieces) but because they start a domino effect where the aircraft destroys itself. Possible scenarios include:

- the explosion blows several holes in the skin, as described above, in such a way that they are opened further by pressurization or aerodynamic forces until the aircraft structure fails;
- the explosion destroys critical components causing safe control to be lost; and
- material ejected from a hole caused by an explosion damages critical aircraft components.

Some technological options discussed in the U.K. report (and elsewhere) include:

- modifying cargo containers to absorb shock waves, prevent fragmentation, and vent overpressures to prescribed pathways;
- adding cargo bay liners to keep fragments from penetrating the cabin floor or fuselage;
- incorporating blow-out panels on the fuselage at container vent positions to control skin ruptures and limit skin tearing;
- closing cavities and pathways that exist between cargo containers and inside aircraft structures (e.g., between floor beams); such cavities can serve as conduits for shock waves and supersonic gas flows, permitting damage at aircraft locations far removed from the explosion site; the U.K. investigation decided that cavities played a role in the Lockerbie incident; and

[23]Department of Transport (United Kingdom), Air Accidents Investigation Branch, Aircraft Accident Report, February 1990: *Report on the Accident to Boeing 747-121, N739PA at Lockerbie, Dumfriesshire, Scotland on 21 December 1988,* p. 58.

. using energy-absorbing material (e.g., in the cavities) to attenuate shock waves.

These options entail numerous cost and engineering problems, including design difficulties stemming from the potential variations in charge size, location within the aircraft, and the nature of the materials in the immediate vicinity of the charge.[24] The combination of engineering and recertification efforts required to structurally modify a commercial transport would likely make most of these options prohibitively expensive. Moreover, some of these options would add to the aircraft weight or reduce cargo and passenger loads, in either case reducing profits by cutting revenue or increasing fuel costs. These options will be more practical in the distant future, if they can be incorporated in aircraft during the design process. The FAA is examining this option.

RESEARCH AND DEVELOPMENT

The FAA has researched the effects of explosives on aircraft in the past, with the focus on where to place an explosive device discovered onboard an aircraft during flight to minimize the catastrophic potential. Also, tests were done on baggage containers to estimate the size of the explosive charge used on Pan Am 103. Recently, FAA held a conference to discuss R&D into examining the aircraft hardening issue. A program along these lines has been implemented at the FAA Technical Center. The following points emphasize the cooperation with outside experts that can be brought to bear in the problem:

- Coordination with military researchers and engineers is valuable (survivability studies have been done on virtually all military aircraft—data on transports would be applicable to airlines). FAA is proceeding to investigate the issue of aircraft vulnerability and hardening in cooperation with the Air Force's Wright Aeronautical Laboratories, the Naval Surface Weapons Center, and the Defense Advanced Research Projects Agency. Experimentation with explosives tests is continuing.
- Aircraft manufacturers also have expertise and technology to address explosive decompression problems, although they are reluctant to discuss it; FAA issued contracts during the 1980s to aircraft manufacturers to analyze the optimal on-board location to place a discovered bomb (to minimize potential damage) for each aircraft type flown by U.S. airlines.
- Coordination with FAA aircraft certification officials and airline maintenance and engineering people would be advisable in attacking this problem, so that the R&D efforts focus on concepts that have the hope of economic feasibility.

The FAA is currently assembling its research and development program in aircraft hardening and survivability and is cooperating with aircraft manufacturers in applying computer codes on structural failure to the problem of on-board explosions.[25]

BIOLOGICAL AND CHEMICAL DEFENSES

The confined space and recirculated airflow within airliners could increase the effectiveness of chemical or biological agents. Many (although not all) biological agents take many hours to produce symptoms. However, chemical attacks as well as attacks with very fast-working biological agents could well be a terrorist option. Few possibilities exist for dealing with this problem beyond attempting to detect the agents when being brought on board-and this would be difficult to do. For aerosols, a separate air system for the flight deck to insulate the flying crew from the effects of the gas would be one tactic. Controlled, but rapid, depressurization in the cabin, to be followed by repressurization, might mitigate effects on the passengers.

ACCESS CONTROL AND EMPLOYEE SECURITY AT AIRPORTS

Access Control

On December 7, 1987, a recently dismissed Pacific Southwest Airlines employee used an ID badge (which was not collected upon his dismissal) to circumvent security checkpoints and board a flight. While the flight was enroute he shot both the pilot and copilot, resulting in a crash and the death of all 43 people on board. One Federal response was

[24]Ibid., p. 54.

[25]Lyle Malotky, FAA, personal communication, April 1991.

a rule[26] **that** emphasizes technological solutions to the problem of unauthorized access. Each commercial airport operator is required to implement a "system, method, or procedure' that ensures that only authorized persons have access to secured areas of the airport. While the rule does not specify the technology choice, FAA's intent was that airports install computer-controlled card access systems.

Airports and airlines have found fault with this rule since its initial proposal in March 1988. The main concern of the airports is *avoiding FAA enforcement penalties.* Institutional problems (coordiation between FAA and other Federal agencies that must operate at airports-Customs, INS, Agriculture; FAA regional differences; state and local employment and privacy laws) cause many of the security management difficulties for airports. Airline management and pilots are concerned that the hodgepodge of airport access/control systems being deployed in response to the rule will hamper operations and raise the fees airlines must pay for airport services. Issues include how to deal with itinerant aircrews (single access card for whole crew used at some airports, escorts used at others-airline control of airport badges); overlap of some airline ''exclusive use areas"; need for some form of a national system-one proposal was a $15 million communication system to handle transient aircrews for all domestic airports but this was rejected because airports are unwilling to pay for transient benefits.

Some sections of the FAA recognized that problems could arise from incompatible access systems used at multiple airports-in an early version of the rule, FAA inspectors (who travel to many different airports as part of their duties) would have been allowed to circumvent computer-card security systems. Vehement airport and airline protests caused the FAA to drop this provision.

Passenger airlines already accomplish a significant access control function-passenger and baggage screening. But cargo airlines are not covered under the same security rules as passenger carriers (14 CFR 108) and consequently cannot be given security authority like the passenger carriers. Therefore the airport must remain responsible for security at cargo facilities, increasing the difficulties in meeting 14 CFR 107.14 access control requirements, a problem for both the airport and the airline.

Background Checks

An additional problem lies in the difficulties associated with checking on the backgrounds of airport employees with access to sensitive areas. The Aviation Security Improvement Act of 1990 permits airport authorities or airlines to check on the backgrounds of prospective employees, who would have access to aircraft. However, authorization is given only to receive information on convictions for certain serious felonies, such as murder, robbery, and rape, that transpired during the previous 10 years. Records of convictions for other crimes or earlier convictions would not be available to the employer.

Currently, up to 90 days are needed for this information to arrive from the Federal Bureau of Investigation. A prospective job applicant may not always be willing to wait this long before accepting a job, which makes it harder to hire. If the applicant were hired in the interim, dismissal after 90 days on receipt of a bad record might induce the individual to use the knowledge acquired to sabotage airport operations. Further, the records are sometimes up to 2 years out of date. Such delays can, in principle, be remedied. For instance, new hires at Baltimore/Washington International Airport have their records in the State of Maryland checked in a matter of minutes. It would be possible to improve on the current nationwide system, at least for a subset of reporting States.

A further problem is the question of current employees. If someone has worked at an airport for years and proved reliable, should a past conviction require termination? Currently, all present employees must be investigated. If nothing else, this will create an enormous backlog in background checks. Some decisions may need to be made on circumstances in which employees of long and good standing might be permitted to remain without undergoing such checks.

To improve airline security and implement an integrated security system, it would be desirable to check in a better fashion on the trustworthiness of employees with access to aircraft. This might mean checking for more than just serious felony

[26] 14 CFR 107.14.

convictions (although complete background investigations, such as now done for those with jobs that require access to national security information, would probably be impractical). For example, other felony convictions or serious misdemeanor convictions could be relevant. Even if a person has no violent history, past dishonesty could raise questions of susceptibility to bribery or blackmail. This situation could be used by terrorists as part of a plan to sabotage aircraft.

To reduce negative impacts on individual privacy, a clearinghouse might be established to receive information on individuals, with only the minimum necessary data passed on to the employer.

Finally, steps must be taken to speed the process for accomplishing the checks.

THE ROLE OF HUMANS IN PROFILING AND SCREENING

Chapter 5 contains a detailed description of human factors and their role in airline security. This section presents a summary of some contributions that this field can make in the specific areas of security profiling and screening at airports.

According to the Presidential Commission on Aviation Security and Terrorism, human factors in the implementation of an airline security system have not received the attention that they deserve.[27] OTA concurs with this observation. A major application of human factors concerns the type of personnel (and their responsibilities and training) utilized in the security system. In the United States, they are often minimally trained, unmotivated, minimum wage personnel, usually working for a contract security services firm, performing boring and repetitive work in a very low-threat-frequency environment. On the other hand, the Israeli model relies heavily on maximum human involvement by a highly trained and motivated force. It is generally agreed from the investigations of the Pan Am 103 accident that better use of security personnel is in order.[28]

The most controversial use of security personnel is in the screening or profiling process that is used to determine which passengers constitute a potential threat and therefore should be given greater scrutiny. However, human factors are also a major factor in the selection and even the design of detection systems (i.e., whether they should be totally automatic, as required by the current FAA EDS rule) and in specifying the degree of automation and human interaction desired. Techniques currently under development, such as the pattern recognition discussed above, can sharpen the attention of screeners in the x-ray image observation process.

When it comes to screening or profiling passengers, the techniques employed by the security division at Ben Gurion Airport in Israel are probably the most stringent. In fact, selection criteria for extended interviews used in Israel could probably not be used in the United States. At this airport, which has just under 20 percent of the international enplanements that occur at Kennedy Airport in New York, a highly motivated and well-trained security force of mostly college-age personnel perform a personal, in-depth interview and profile evaluation. The profiling depends on the travel documents (the airline tickets and passports) plus responses to a set of questions, but most importantly, the integrity of the security system depends on the observations and the personal initiative of the highly trained staff. The aim of this process is to eliminate a large fraction of the passengers, who do not appear to represent any possible threat, from the time-consuming, thorough search process and to select only that small segment of the passengers who for any reason present some suspicions for such a search. The other passengers are allowed to proceed through security with a minimum of surveillance and only a few questions about their checked baggage. However, there is a further, last-minute positive baggage match of all passengers and all checked luggage at the entry point to the aircraft. No flight leaves with a piece of unaccompanied baggage that has not been thoroughly searched for weapons, explosives, or other contraband.

A number of U.S. airlines (e.g., American, Trans World, and Pan American) have employed Israeli consultants with knowledge of these techniques to devise similar programs, tailored for their operations, as well as to train their personnel. The standard

[27] The White House, the President's Commission on Aviation Security and Terrorism, op. cit., footnote 21, p. 122: "The FAA must take the lead in stressing the role of human factors in the security equation; training must be improved."

[28] See, for example, the White House, the President's Commission on Aviation Security and Terrorism, op. cit., footnote 21.

argument against the Israeli approach is that it is too expensive (22 percent of the Ben Gurion Airport operating budget goes to security), that it is too time-consuming (passengers are requested to be at the airport 2 to 3 hours prior to departure time), and that it is too disruptive. Most of the consultants are attempting to devise systems that will overcome these shortcomings without compromising the quality of security.

The FAA has been experimenting with a semi-automated profiling system, the Comprehensive Passenger Screening Profile (CPSP), in which the security person keys the answers (yes/no only) to a set of 7 questions into a portable computer terminal, which then compares the answers against a database and produces a risk assessment. The operator uses the results to dispose of the case. The system constantly adds new data to an original, intelligence-based, database of the profiles of threatening passengers for future use by both the airlines and the FAA. The FAA is considering making the CPSP mandatory for all U.S. airlines, and, as an incentive to the airlines, the FAA has offered to assume liability for failure to detect: airlines can blame the FAA if the system fails to detect an actual security threat. However, some airlines have objected to sharing their passenger profile data with the FAA.

The incorporation of an effective profiling system into an overall security system could eliminate a large number of passengers from further screening. To date, the FAA has considered profiling apart from the overall security process and has not included it in considering the performance requirements of detection equipment. In fact, the definition of the screening system has been handled by the FAA Aviation Security Division intelligence group, quite separate from those responsible for security R&D. Profiling makes slower, more complex detection systems more interesting in high-traffic situations, where they could not possibly handle all the items arriving at the check-in counter. Incorporation of profiling is another argument against setting throughput standards for detection equipment at the R&D stage. The Xenis EDS at Gatwick Airport near London, has been used with a profiling system that requires only a small fraction of the baggage to be viewed by the TNA.

Human-factors design has also proven useful in the process of heightening the attention of security personnel operating repetitive and boring tasks such as viewing the x-ray images. One vendor (EG&G-Astrophysics) has produced a false alarm data package (a cassette or disk) that randomly superimposes various threat objects on the images of luggage on the viewing screen.[29] The operator can attempt to clear the threat by pressing a key if he/she recognizes it (the program clears the threat unless it is real). An operator who fails to do so can be disciplined. This technique can also be used as a positive reward system for all threats "caught."

The degree of automation that is demanded of a detection system is another human engineering consideration that must be considered at the design or even system conception stage. The human brain can often be the most powerful discriminator, especially when well-trained personnel are involved. The use of an automatic system to alert the human operator of a suspicious situation is a powerful tool. This is actually the way in which the Xenis was used in the tests at Kennedy Airport. There was always an operator who made the decision whether to call the passenger to open the bag when the Xenis signals showed an alarm. In this way the automatic system is used to counter a major human fallibility, lack of attentiveness, rather than replacing the humans. At the Gatwick tests, however, if the machine alarms, the operator cannot overrule it, and the bag is automatically given careful scrutiny by security personnel, usually including a hand search.

COMBINED USE OF SEVERAL DETECTORS WITH PROFILING

Choosing a practical architecture of detectors to provide the best possible security system is an important challenge. Such an analysis should be performed for various levels of detector technology: current state-of-the-art, likely near-term capability, and long-term potential.

A problem with such an effort is that the necessary performance data on various candidate sensors is not available, and consequently any such effort must, at this time, depend on guesswork and conjecture. However, even an attempt to perform such an analysis would be informative.

[29] This was funded under the FAA Small Business Innovative Research program.

Appendix C of the National Academy of Sciences study presented a hypothetical example of a detector system architecture for illustration. It focused on the cost of the overall system but left out the connection to possible solutions that may meet the requirements of the various stages.

The following discussion is not meant to provide an optimal architecture for a combined explosives detector system. It is only an example presented for purposes of illustration.

From a systems point of view, the sensitivity always gets worse in any cascade of detectors and only the false alarm problem can be improved by the repeated use of AND gates (see discussion in section on statistics, above). It has been generally accepted that the overall detection probability of any chosen system should be high (at least 0.85, or so). This means that the individual detector P_d's must be very high, higher than 0.90, in order to yield this overall system performance. Three stages, each of $P_d = 0.90$ would result in an overall P_{dc} of only 0.73, which might not be considered acceptable.

It follows that, for several stages operated as an AND gate, it would be desirable to use individual detectors with detection probabilities that are close to perfect, on the order of 0.98 to 0.99. There is currently nothing known that can claim such sensitivity, the R&D programs are not even directed at achieving such a high value, and current test protocols are not capable of determining whether such a value has actually been achieved. On the false alarm side, the objective of a combined system should be to bring the need for final hand search down to a number of bags that can be handled by one or several security personnel per given station. Allowing for 5 minutes per hand search, one should thus look for systems that would not require more than 12 to 24 bags per hour to be hand searched per station. In a situation with very high throughput, such as exists at some of the major international airlines at Kennedy Airport where the throughput can be as high as 4,000 bags per hour, this would require an overall false alarm rate of about 0.5 percent. It is interesting to note that three independent stages, each operating at a false alarm rate of about 20 percent would almost be able to meet this requirement (0.8 percent v. 0.5 percent).

A possible system might thus *theoretically* consist of three different stages of detection equipment all operating with P_d approximately 0.97 and F_a about 0.20. The first would be a high-throughput stage (this stage may have to be a number of parallel inexpensive detectors), the second stage could be of more moderate speed and possibly somewhat more expensive, and the last stage could be quite slow and possibly expensive, since a single unit should suffice due to the smaller number of bags handled. It is worth repeating that the multiple detector approach puts the strain on achieving very high sensitivity (high P_d) at each stage, while allowing for much more relaxed false alarm criteria than if a single stage of detection is utilized. It is not clear how close this ideal will be approached in the foreseeable future.

The characteristics of the frost-stage screening detector are very critical since it must handle the largest throughput of luggage. In a high-throughput situation, such as encountered by some of the major airlines at the major gateways, this is a demanding requirement. The candidate detectors for this use should be as inexpensive as possible, since it is likely that many or several parallel detectors maybe required to handle the traffic. For instance, the FAA requirement of a throughput of 600 bags per hour for the EDS still would demand as many as 5 to 10 systems in high traffic. This strongly argues against the use of expensive systems such as the SAIC/TNA as a first stage.

Probably the primary candidate for a first-stage screen is a well-designed, thorough, profiling system operated by motivated, well-trained security personnel. Profiling systems typically identify a few percent of the sample as potentially threatening and requiring further investigation (the actual percentage is very situation- and process-sensitive). It is extremely difficult to identify a quantitative detection probability and false alarm rate for a profiling system.

Another measure, which is not specifically a detection stage but should be a part of any overall system, is a foolproof, positive, passenger/baggage match for all boarded passengers to prevent the shipment of any unaccompanied baggage (unless baggage separated from passengers-e. g., by airline error-is subject to specific stringent security measures). Such a system would raise the stakes for any terrorist group, by isolating the potential threat to dupes who do not realize that they are carrying a bomb, or suicidal terrorists who are willing to sacrifice their own lives.

When it comes to existing detection hardware, advanced x-ray imaging systems will probably be a significant component of any integrated security detection system. Included among the advanced x-ray concepts for consideration should probably be the T-Scan™(dual-energy, dual-view), Z-Scan™ (backscatter) systems, and probably other similar systems including those that emphasize pattern recognition. These systems all have some ability to detect masses of materials with low atomic number that could be explosives but could also be many other common materials. They should be effective in identifying electronic hardware, which have been popular hiding places for explosives in the past. A recent assessment of the capability of certain of these systems for this specific purpose has been conducted by the FAA Technical Center.[30]

Currently, the performance of these systems when used in realistic environments is not known. It is quite possible that the specificity of these systems is quite high, but the false alarm rate is a completely unknown factor. How many suitcases contain some sort of electronic equipment that would require the security inspectors to take a second look? How many other objects with low atomic number would be mistaken as explosives? Could the false alarm rate of such a system be kept in the 20-percent range?

Some advanced x-ray systems, such as the American Science and Engineering (AS&E) Z-Scan™ concept, could be particularly sensitive to the popular terrorist technique of lining a standard suitcase with a thin layer of Detasheet-like explosives inside the normal lining. The Z-Scan™ has somewhat limited penetration capability but is very effective at or near the surface facing the x-ray source, and consequently, with its double-sided illumination, it should be especially sensitive to explosives hidden in the lining.

There has been some recent interest in coupling vapor detection sniffers with advanced x-ray systems used in the above manner to detect electronics and other threatening masses. In this coupling, the sniffer is used only on those items identified by the x-ray system as presenting a potential threat. Thus the vapor sniffer has the specific role of detecting explosive particles or vapors on electronic components and of differentiating low-Z (low atomic weight) masses that are made of harmless materials. Any vapor detector, no matter how good, is always susceptible to the technique of sealing the explosives in impervious wrappers; however, there has been great controversy about the practicability for terrorists to achieve this level of cleanliness.

A candidate for the final detection screen could be the x-ray CT scanner currently being developed by Imatron. With the CT scheme, it is possible to determine the mass density of each volume element due to the many cuts being taken through the same element. This knowledge, combined with the excellent spatial resolution inherent in the CT system, allows for a automated identification of masses that have both the correct density and a suspicious shape. Further, the suspect region identified automatically can be viewed by the operator in a three-dimensional reconstruction from various aspects. Although the ability of this scheme to identify unambiguously the various candidate explosives has not yet been demonstrated quantitatively, the primary shortcoming of this scheme is the questionable speed of the system. The speed is a function of the time required to achieve one slice through the suspect object as well as the number of slices required to achieve the needed resolution for three-dimensional reconstruction.

Currently, the prototype system at Imatron requires about 6 seconds per viewed slice of l-cm thickness, with the promise of being able to reduce this to 2 to 3 seconds. The number of slices required is a more subjective issue and depends also on what information is available before the CT scanner is utilized. In one current scenario, an advanced x-ray system might indicate the presence of a suspicious mass in one quadrant of a luggage piece, thus allowing the search to be conducted over a restricted predetermined area. If one then assumes that 6 to 10 slices are required (there are no published data on this question), it follows that current technology might require about 1 minute per bag, while there is hope for reducing this time to 10 to 15 seconds. In a third stage detection application, where the flow of baggage may have been reduced to roughly 4 percent of the total throughput, one device may be able to handle the high-throughput requirement of most of the high-traffic airports (i.e., operate at about 1 or 2

[30]At this writing the results of this assessment have not been publicly released by the FAA, but it is understood that the vendors have been informed as to the FAA assessment of the performance of their hardware.

bags per minute). Such a system may leave very few bags to be opened for hand inspection.

It is also possible that the current SAIC/TNA system could serve the purpose of the third stage detector in a multistage detection system. Since the throughput of a third-stage system could be relatively modest even for highest traffic use, it maybe possible to achieve somewhat better performance by slowing down the SAIC/TNA system from its current 6-seconds-per-bag goal.

From the above discussion, it maybe possible to synthesize a multistage explosives detection system, based on current or near-term technology, by guessing reasonable performance values for the systems used where the data are not available. First, the system should have a positive passenger/baggage match for each flight segment, which, however, does not affect the performance. The first detection stage could be profiling with a false alarm rate of 0.05. The main shortcoming of the use of profiling at this position in the system is that it is not the ideal, cheap stage, since the personnel requirements, and consequently cost, for this process are high. Furthermore, its detection probability is unknown.

In addition, the first stage could contain an advanced x-ray system, automated to respond to low-Z masses and electronic hardware. It is possible that such a system might operate with high detection probability, but would have a significant false alarm rate, perhaps 0.20. The cost of the x-ray system could be between $50,000 and $200,000 each. For the purposes of this analysis, the assumption of a 0.90 P_d is used.

All items alarming the first stage would be passed to a second stage, which could be a vapor detector. The vapor detectors could be collocated with the x-ray system or could take the luggage from several such stations. Vapor detectors might operate at a relatively high P_d and a false alarm rate of 0.20, provided that the luggage had been previously screened by the x-ray system. Again, for the sake of the argument, the optimistic assumption of a P_d of 0.95 is made. Vapor detectors that show some promise are on the market now. There is considerable variation in their cost: $50,000 to $150,000 per station is an approximate range.

The final stage could be an Imatron CT scanner. If enough time were available and enough cuts are taken, the detection probability of this system might be very high, say 0.95 to 0.98, while the false alarm rate could be quite moderate. An estimate for this discussion is 0.10. The CT scanner would probably cost about $500,000 to $700,000.

In a high-traffic situation (like TWA at Kennedy Airport) of about 3,000-4,000 bags per hour, such a system might consist of one to three Imatron CTs (depending on whether they can process one or two bags per minute), which would result in about 10-15 bags per hour being hand searched. The second-stage devices would need to handle 150 to 800 bags per hour (depending on whether the first stage is a profile or an x-ray system). If we assume that a vapor detector requires 30 seconds per bag, three to seven such detectors would be required.

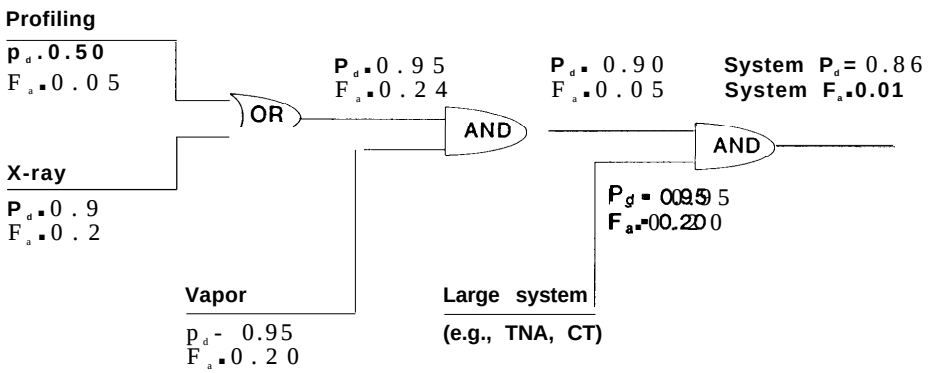
The first-stage x-ray detectors have a fairly high throughput. Current systems can easily handle 600 bags per hour. If we assume that the data processing will not slow down the systems, it might take about six of these systems to handle the high traffic.

As far as cost is concerned, using the lower range figures, this complete station would cost about $1,00,000 in equipment, while the upper end might be as high as about $4,000,000. This would be less than the cost for 19 TNA machines (probably over $20 million for capital costs), thought necessary for Kennedy Airport in the absence of other technologies for explosives detection. The overall detection probability, P_{dc}, would be 0.81 to 0.84. The false alarm rate would be 0.004 (if all devices were statistically uncorrelated, which is probably not strictly true). Although we have had to assume the performance values used in this example, it does give hope that respectable detection performance might be achieved with near-term hardware.

An improvement on this technique (see figure 4-2) would be to begin with an OR gate, combining profiling and the first x-ray screen. An alarm on either technique (or both) would send the bag on to the more sophisticated detectors. That way, failure by either profiling or x-ray alone would not cause the system to fail as a whole. The x-ray device might be a backscatter machine, or a refined dual-energy system. Both types of detectors react to high-density items of low atomic weight, like high explosives. The advantage of x-ray systems over TNA for a first stage is in the cost, which is a factor of 5 to 10 less.

The detection probability for profiling is unknown; it is certainly greater than zero. The Murphy

Figure 4-2—Notional System Combining Different Explosives Detection Technologies



SOURCE: Office of Technology Assessment, 1991.

case in London-among others-where an El Al security agent discovered, through interviewing and then examination, a bomb placed in an unsuspecting woman's carry-on luggage by her terrorist boyfriend, attests to that. It is certainly less than 1.0, evident through common sense and through some experiences that have indicated the rare passage of bombs through a careful profiling system. By using an "OR" gate between profiling and a good mechanical system, the system would scrutinize a bag that fails *either* technique, resulting in a detection probability greater than that of either alone.

As an example, if the x-ray system had a detection probability of 0.90 and the profiling one of 0.50, the combined system would have a probability of 0.95 = (0.90+ 0.50– 0.90 * 0.50);[31] if the profile has a better detection probability, say 0.80, the overall probability is better, too-O.98; and if the profiling doesn't work at all, the system still retains a 0.90-detection probability. The false alarm rate of the profiling is set by the user, generally at 0.02 to 0.05. If the false alarm rate of the x-ray device were high (say, 0.20) the combined false alarm rate would be 0.22 to 0.24. This would mean that 22 to 24 percent of the luggage would proceed to the next level of scrutiny.

Following this stage, one could add another stage with a totally different technology, say, a vapor detector, which would be especially appropriate for carry-on baggage. In this context, assume, again optimistically, that the vapor detector had a detection probability as high as 0.95 with a false alarm rate of 0.20. Finally, one might add a TNA or a computerized tomography system. Assume for this system as well a detection probability of 0.95 and a false alarm rate of 0.20. These numbers are consistent with or more conservative than earlier proposed FAA criteria for acceptability of single explosives detection systems. The combined detection probability of the system is relatively high (0.86, assuming only 50 percent effectiveness of profiling and the false alarm rate is low (about 1 percent). Excessive reliance on one technology (the first-stage x-ray) would be reduced using OR gates with profiling.[32]

CARGO AND AIRMAIL

To be complete, a security system would have to protect against bombs being brought aboard aircraft through the cargo route. At least two countries, Switzerland and Israel, currently employ a variety of techniques to counter this eventuality. These include delaying shipment of packages and exposing them to the altitude profile of the flight by subjecting them to depressurization, extra use of x-ray equipment for examining packages with care, and special equipment for probing packages that are suspect. Switzerland also has special equipment for examining mail

[31]This assumes *that* there is no correlation between the two techniques, profiling and x-rays, as app

[32]Again, this assumes a perfect situation in which there is no correlation among the different detection systems This will not be true, although the correlation will often be quite small, so the combined probabilities and false alarm rates should be close to the theoretical ones cited in the text.

bound for "high-risk" destinations, such as the United States and other Gulf War Coalition countries. Special x-ray equipment and other means of examining packages are used.

In the United States, where the volume of air traffic is much larger than in the above two countries, the FAA is considering several possibilities for increasing security of air cargo. One approach would be to require forwarders to open and inspect shipments from sources unfamiliar to them. In addition, FAA now requires that international shipments to the United States handled by on-board couriers be x-rayed before the couriers board the aircraft. During the Gulf War, the U.S. Postal Service shifted all mail, except for the smallest parcels, to all-freight flights. In another development, British Airways is planning to install x-ray machines at U.S. gateway airports to check small and express shipments for explosive devices.

SUMMARY AND COMMENTS

The fundamental problem in explosives detection is to design an EDS that has acceptable detection probability and false alarms rate but does not unduly inconvenience travelers. One approach is to combine detectors based on different phenomenologies to provide independent assessments of whether items boarding an aircraft contain explosives. A suggestion for such a system has been presented. The need for a detailed systems study to optimize such a system has been recognized by the FAA Technical Center and a research program to this end is underway.

An approach synergistic with the first is to harden aircraft, raising the amount of explosives needed by the terrorist, and making detection correspondingly easier for counterterrorist systems. Research in this direction is being pursued; first indications of the promise of this line of work will not be known for at least a year or two.

In addition to detecting explosives brought aboard by passengers in checked or carry-on baggage, a complete system would have to prevent passengers from carrying explosives on their persons and to prevent explosives from being hidden among cargo or secreted on the aircraft by personnel with unescorted access to aircraft. Some vapor detectors, x-ray microdose, or radiofrequency methods of explosives detection may solve the problem of explosives carried by passengers. As for mail and cargo, the bulk methods of detection (x-ray and nuclear) could be engineered for this application at current levels of technology. Also, delay and depressurization of cargo (as done in Switzerland and Israel—following the altitude and time profile of the specified flight) could be used to detonate cargo bombs in bunkers on the ground. Wider systems studies, such as those being done at Baltimore/Washington International Airport, would also help in solving these problems.

Finally, in designing security systems, it would be advisable to "red team" individual devices and entire systems. That is, the FAA might arrange for outside experts to consider how a device or system might be circumvented, to assess the ease of doing so, and to consider countermeasures against circumvention. This information would be helpful both for the FAA and any outside testing evaluators[33] in deciding what kinds of systems are acceptable, and for airport operators and airlines to understand better their security capabilities.

[33]See again finding 4 regarding outside testing in chapter 1 of U.S. Congress, Office of Technology Assessment, op. cit., footnote 2, pp. 8-10.

Chapter 5

Human Factors in Aviation Security

Contents

Box

Chapter 5
Human Factors in Aviation Security

INTRODUCTION

Human resources are critical to aviation security. Security personnel—passenger and baggage screeners, guards and law enforcement officers, and airport and airline employees in general-are important elements of a system that prevents and deters hostile acts against air carriers. Technology can enhance, but cannot replace, the capabilities of these people and the many services they provide. Moreover, management practices based on behavioral research findings can further improve human performance.

This chapter considers the function of screeners in weapons and explosives detection, and the role of guards, officers, and other aviation employees in discovering (and deterring) suspicious individuals or situations. Within the past 20 years, technology has greatly increased the capability and productivity of these security people. Metal detectors and x-ray devices are faster, more accurate, and more socially acceptable tools for screening passengers and baggage than manual searches. Remote television and other monitoring devices, computer-controlled access to restricted areas, and communication and data systems allow comprehensive surveillance and threat assessment. While these technologies raise the capabilities of a security system to new levels, their ultimate success and actual performance depend on the people who design, operate, and maintain them.

Many security assignments require repetitive tasks and close monitoring for rare events—functions that humans perform poorly. Selecting well-suited individuals, training them properly, designing their work environment and rotation schedule to elicit the best possible performance, and providing motivating incentives are fundamental requirements for successful operations, regardless of the type of technology in place. These functions involve human performance; application of human factors in these cases can greatly improve the utilization of technology for airline security.

Dramatic accidents caused by human errors in the nuclear power, chemical, and transportation industries have increased public attention to human performance issues during the past decade. Additional training requirements, revised operating procedures, warning devices, and expanded government oversight are typical recommendations following accident investigations. However, these stopgap measures address only the surface of problems that are rooted in the complex interactions of people and equipment within the larger system and the institutional and organizational structures and procedures that drive the planning, design, and management of these systems. Following the ground collision of two jetliners in Detroit in December 1990, Dr. John Lauber, a member of the National Transportation Board, said that "basically the [aviation] system, the way we're operating it, almost demands nearly error-free [human] performance. ' Similar concerns can be echoed for the aviation security system—a number of successful airline terrorist events have been traced to a human failure.[2] "The challenge is to design a system. . which is tolerant of those errors when they do occur and which detects and traps them before we have [a catastrophe]. "[3] Multilayered defenses are employed at many commercial airports and airline terminals, and security managers and government authorities are turning to new technologies to buttress these systems. Heretofore, Federal requirements and industry use of security technologies have usually been with specific functions in mind. As long as the technical goals could be met effectively, the equipment was considered satisfactory and human performance problems related to the technology were resolved through revised training and procedures. Technology use in counterterrorism will likely increase dramatically over the next decade, but if early and

[1]John Lauber quoted by John H. Cushman, Jr., "Test for Aviation: Coping with Human Shortcomings," *The New York Times,* Dec. 10, 1990, p. A17.

[2]One example was the destruction of a Korean Air Lines flight over the Andaman Sea by a bomb planted by North Korean agents. The device, in a carry-on bag, was ahnost detected at a security checkpoint in Baghdad at an earlier stop. When a security guard wished to remove the batteries from a radio, one terrorist turned the radio on, proving it operated, and then raised a hue and cry, yelling and complaining. Instead of using this as a reason to stop the two suspect individuals and to examine their belongings minutely, the security forces decided to avoid trouble by allowing them to proceed.

[3]Lauber, op. cit., footnote 1.

methodic attention is not given to human performance issues, we may expect that system efficiency and effectiveness will be substantially impaired.

Background on Human Error

The human role in a security system is complex; thus the nature of human errors, from mental to physical, varies widely. Mental or cognitive errors can include improper judgment or decisionmaking, while physical errors may stem from motor skill deficiencies or faulty equipment design. A combination of physical and mental processes may influence other kinds of errors, such as those involving communication, perception, or alertness.

Human factors, a discipline combining behavioral sciences and engineering, focuses on improving the performance of complex systems of people and machines. Designing and operating a system so that it does not induce human error (in fact, designing it so that human error may be minimized) is one critical component of human factors and limiting the impact of a human error once it occurs is another aspect.

Many types of human error are systematic, following certain predictable patterns; once these patterns are identified, countermeasures can be developed. For example, poor location of switches or dials can induce manual or perceptual errors. For those types of human error that do not follow predictable patterns, mitigation techniques are difficult to develop. Some examples of mitigation techniques include automatic monitoring and warning devices. These subsystems, when properly designed and implemented, can be invaluable tools for negating human error.

Employee selection—allowing into the system only those people least likely to make mistakes—and continued quality control maintained through training and monitoring are basic steps for minimizing human errors. Potential errors can be forestalled by the use of standard procedures and checklists for routine and emergency tasks, planning work shifts and assignments so as not to induce inattention and fatigue, and properly designing the work environment. "If human factors engineering is done properly at the conceptual and design stage, the cost is high, but paid only once. If traning must compensate for poor design, the price is paid every day. "[4]

According to one expert, there does not appear to be a strong need for new basic research in human factors related spectifically to security-behavioral science findings in general and experience with human performance problems in other industries are probably sufficient to enhance current security operations.[5] For example, such knowledge is being used to upgrade security screener selection by airlines, and to improve training standards. However, the mechanisms to identify early on and to address effectively the human performance issues stemming from new security technologies, such as explosives detection systems, are not yet in place in industry or the Federal Government.

Shifting boring and repetitive tasks that people perform poorly to machines is an approach that can reduce errors. However, automated devices (or any new technology) may create new sources of human error.[6] Excessive false alarms unnecessarily distract operators and may lead to the device being ignored or disabled. During unusual or emergency circumstances, the lack of flexibility in many automated systems can be a serious limitation and the human backup may not be mentally or physically prepared (or possibly even capable) to take over. Consequently, a full system approach is required for reducing total human errors.

FAA AND HUMAN FACTORS

FAA Policy and Plans for Human Factors and Aviation Security

In a report released in July 1988, OTA concluded that FAA attention to the spectrum of human performance problems in commercial aviation fell far short of the level warranted, since human error is the leading cause of aviation accidents.[7] Later that same year, Congress passed the Aviation Safety

[4]Earl L. Wiener, "Cockpit Automation' *Human Factors in Aviation*, Earl L. Wiener and David C. Nagel (eds.) (San Diego, CA: Academic Press, Inc., 1988) p. 454.

[5]H. Clayton Foushee, Chief Scientific and Technical Advisor for Human Factors, FAA personal communication, 1991.

[6]See Wiener, op. cit., footnote 4, ch. 13 for a discussion of new and subtle types of human error that have resulted from the introduction of automation into aircraft cockpits.

[7]U.S. Congress, Office of Technology Assessment, *Safe Skies for Tomorrow: Aviation Safety in a Competitive Environment*, OTA-SET-381 (Washington, DC: U.S. Government Printing Office, July 1988).

Research Act, which directed the FAA to expand its research efforts on human performance in aviation and authorized funds specifically for that purpose.[8] The FAA responded by creating the position of Chief Scientific and Technical Advisor for Human Factors, responsible for coordinating for the FAA various human-factors research efforts within the FAA NASA, and the DOD and for opening lines of communication within the FAA and industry. Communication among Federal agencies is critical, since decisions made by the aviation industry and the operational and regulatory sections of the FAA often drive the need for new human-factors research and could benefit from an understanding of human-factors research findings and products.

The FAA has made progress in addressing the earlier criticism of its human-factors programs and understanding in aircraft and air traffic control (ATC) equipment and operations. However, the key shortcomings in FAA human-factors efforts that OTA cited in its 1988 study-insufficient agency expertise, uncoordinated research efforts, and regulations and certification standards that do not reflect human-factors principles-still exist within FAA civil aviation security programs. During the course of its study, OTA examined closely many of the technology development programs and regulatory efforts underway in the security sections of FAA and found a general lack of awareness and understanding of the human-factors issues involved with possible new security technologies. An exception to this situation, however, and a hopeful indicator of a new trend, has been the hiring of a human-factors expert at the FAA Technical Center to oversee human-factors research as it relates to airline security.

However, at present, it appears that the FAA is ill-prepared to identify and address possible human-factors concerns with the increasingly complex and diverse security technologies now under development. The dearth of trained human-factors specialists in areas of the FAA responsible for civil aviation security is a serious deficiency. Until recently, the Aviation Security R&D Service of the Technical Center would have merited similar concerns, but this shortcoming is being redressed, at least in part. Some of the expertise that the FAA is developing on human factors for other uses could also be applied to security issues.

One potential vehicle for bringing human-factors knowledge into aviation security efforts is the National Plan for Aviation Human Factors (HF Plan), the first major product of the heightened FAA attention to human performance issues following the enactment of the Aviation Safety Research Act. The HF Plan identifies significant human performance issues and lays out a 10-year blueprint for establishing and coordinating research programs and conveying the results across Federal agencies and industry. The HF Plan's development depended strongly on advisory committees composed of a cross-section of research, operational, and regulatory representatives from government and industry and approximately 50 of the nation's leading human-factors researchers.[9]

The good news for aviation security is that the Plan appears to provide a strong foundation for multi- and cross-disciplinary efforts and understanding in human factors and has begun to institutionalize and focus consideration of human-factors issues in FAA decisionmaking. The bad news is that nowhere in the Plan is security mentioned—the Plan addresses the following five aviation environments only: aircraft flight deck, air traffic control, aircraft maintenance, airway facilities maintenance, and flight deck/ATC integration. This should not be construed as criticism of the general thrust of the HF Plan—the human-factors categories considered have historically been more critical to aviation safety and are considerably more complex than human performance issues in security-and it is beyond the scope of this study to analyze in detail the specifics of the HF Plan. **However, some objectives and products of the HF Plan maybe directly transferable to aviation security, provided that lines of communication are established and security experts are included in committee structures.**

The Plan has eight objectives, all of which can apply to aviation security, but the following two are especially pertinent, given the present attention to technologies for countering terrorism:

. to encourage the development of principles of 'human-centered' automation and the design of

[8]Aviation Safety Research Act, Public Law 100-591.

[9]U.S. Department of Transportation Federal Aviation Administration, "The National Plan For Aviation Human Factors," vol. I, draft, November 1990.

advanced technology that will capitalize on the relative strengths of humans and machines;
. to develop human factors-oriented validation and certification standards for aviation system hardware and personnel that will enhance both safety and efficiency .10

The HF Plan is designed to be reexamined and revised periodically and aviation security could be added explicitly as a focus area if need and resources warrant.

Crucial to the development and future success of the HF pian is the Human Factors Coordinating Committee (HFCC), formed by the FAA administrator in September 1989.[11] HFCC has representatives from each major division of FAA and serves as "an advisory body for senior management of FAA in all matters involving human performance and [is] intended to assure that human factors issues are represented in all FAA activities. ' '[12] Until very recently, the Assistant Administrator for Civil Aviation Security was not represented on this committee.[13] However, this omission has since been rectified.

FAA Requirements for Aviation Security: Human-Factors Implications

Aviation security personnel and equipment have not received (and have not needed) the same level of regulatory and certification attention that the FAA places on flightcrew, air-traffic controllers, and ground support personnel and their respective aviation equipment. The FAA has focused its regulatory efforts on elements of the aviation system essential to flight safety. For example, the performance of pilots and aircraft systems are continuously critical for maintaining safety-a failure could cause an accident. On the other hand, the performance of the security system (other than as a deterrent) is rarely critical-flight safety is at risk only when security performance fails at the same time that a threat occurs. Moreover, FAA staff and the agency "culture" are predominantly interested in aviation technology and operations and protecting facilities and countering terrorism are not an inherent part of aviation.[14] However, the increasing Complexity of screening technologies and the continuing (possibly increasing) terrorist threat make the performance of aviation security systems more critical to flight safety.

Aviation terrorist events in the 1980s made apparent the shortcomings of the minimum Federal security requirements. The FAA and the airlines both focused attention on screener selection and training, detection and screening technologies, and airline management of security programs and systems. The FAA has increased requirements and oversight of security personnel (selection, training, and management) and equipment (weapons and explosives detectors), but has not yet addressed how security personnel and equipment perform as components of a system.

Screener Selection and Training

For years, the people who screened airline passengers and baggage for domestic flights generally received little training, low wages, and few benefits.[15] Consequently, alarming numbers of domestic screeners failed unannounced FAA tests (22 percent failure rate in 1988).[16] Since there has not been a severe domestic terrorist threat against aviation in the United States, these shortcomings have not resulted in life or property losses.[17]

In light of public pressure following the Lockerbie disaster and costly fines stermming from FAA inspections, the Air Transport Association (ATA) developed an extensive set of screener selection, training, and compensation standards. ATA pro-

[10] Ibid., p. 3.

[11] Ibid., p. 28.

[12] Ibid., p. 28.

[13] Under the FAA organizational structure in place in 1988 through 1990, the Office of Aviation Security was represented by the Executive Director for Regulatory Standards and Compliance, to whom it reported.

[14] Knowledge of aviation technology and operations is important to aircraft and airport security. For example, special characteristics of aviation, such as large volumes of people and luggage that must be screened quickly, drive the security system design and functions.

[15] However, airlines customarily have higher standards for security personnel working in international operations.

[16] Lynne Osmus, office of Aviation Security, FAA, personal communication, Feb. 22, 1991.

[17] Depending on the definition, the destruction of a PSA flight in 1987, caused by a disgruntled ex-employee who shot the flying crew in flight, @@t be considered a terrorist, as well as criminal, act. In this case, the ex-employee had an identification card with which he gained access to the aircraft, so screener training was not an issue.

posed that airlines (or their security contractors)[18] consider education and health criteria, the ability to speak English, and aptitude test results before hiring screeners, and that they offer competitive wages, benefits, and incentives and follow a comprehensive training curriculum. In March 1990, the ATA asked the FAA to adopt its proposal as requirements for all airlines. Based on this cooperative industry effort, the FAA has required some of these suggested upgrades in training measures for screeners. (Most U.S. airlines have adopted at least some of the ATA recommendations; the failure rate on random checks has since dropped significantly.)19 The FAA decided not to include selection and wage standards because such a change would require public comment (i.e., through the *Federal Register),* thereby calling attention to perceived or actual security weaknesses.

Management Practices and Human Performance

The FAA mandates certain positions in an airline's organizational structure, such as a security director for the airline and security coordinators at each airport, but airline management practices and philosophy usually fall outside the scope of FAA regulatory authority. In Safe *Skies for Tomorrow,*[20] OTA found that the effect of airline operating or management practices on airline safety, and changes in those practices, were rarely addressed in FAA safety analyses.[21] The FAA's Human Factors plan cites the influence of management "culture" on human performance as one area where basic research is needed.[22] If the organizational "climate" (i.e., working conditions, wages, management, organizational culture, etc.) does not allow an individual to perform at his or her peak, it may not matter how well he or she is trained or how well designed the technology is.[23] The ATA proposal for upgrading screener standards suggests giving screeners employee benefits common in many industries (vacation, holiday, medical) that contractors often don't receive); offering to contractors the advantages of airline employment (e.g., low-cost travel) and career opportunities to top performers; providing monetary rewards to those who detect test weapons and explosives (and even higher rewards to those who find the real thing); and increasing wages to at least the "local prevailing rate." For comparison, in Israel, screeners are paid at a level considered a "good" salary, far higher than minimum wage. In Switzerland, they are paid at the rate of about $lOper hour. In the United States, rates are often near minimum wage.

The United Airlines' approach to improving screener performance on all flights from selected airports delineates one set of management techniques (box 5-A). Another approach has been undertaken by American Airlines, although only for its international flights.[24] American treats its international screeners as part of the American team. They are hired as full-fledged airline employees, not employees of a contracted security agency, and enjoy the same salary levels and benefits that ticketing agents do. The educational level of entrants appears relatively high, with a few individuals having advanced degrees. There appears also to be a real opportunity for advancement within American Airlines, and not just in the security division. Before starting work, the entrants are brought to Dallas (from across the world; many screeners are hired from the countries in which they will be working) for 2 weeks of training at American's headquarters. The training includes emphasis on the screening questions as well as on what to look for on the x-ray screens. The screeners ask the standard questions as to who packed the baggage and whether anyone could have placed contraband in it. But they also ask general questions regarding destination and travel plans, somewhat akin to the lines of questioning performed by El Al. Indeed, American has used Israeli security consultants in designing their security system. The screeners look for a number of specific characteristics, which remain proprietary to the company. If too many of the characteristics match a passenger, the individual's baggage will receive much closer inspection. Screeners are ro-

[18] Most screening for domestic flights in the United States is conducted by security Contractors, nOtairline employees.

[19] Lynne Osmus, op. cit., footnote 16.

[20] U.S. Congress, Office of Technology Assessment, op. cit., footnote 7.

[21] Ibid., p. 88.

[22] U.S. Department of Transportation, Federal Aviation Administration op. Cit., footnote 9, p. 15.

[23] Ibid.

[24] SOURCE: Site visit t. Dallas Airport, December 1990, and Homer Boynton, Chief of Security, American Airlines, personal communication, December 1990.

tated between looking at x-ray screens and interviewing passengers.

Periodically, security systems are tested by contractors, who choose an American employee to play a terrorist. A specific scenario is given to this impostor, and the reaction of the security personnel is noted. If they do not perform their functions, they may be subject to severe discipline, including termination.

The result of the overall approach, using incentives and threat of discipline for negligence, appears to be a well-motivated and alert force.

Security Equipment

Currently, the FAA requires airlines to employ relatively few types of security equipment—primarily x-ray devices and metal detectors. The FAA established minimum performance standards for detecting weapons and explosives, and since these technologies are radiation-based, the FAA also requires that they meet Federal health and safety standards .25 There are no standards governing operator interaction with the equipment, such as the layout of controls and display symbology options. At the time the FAA established x-ray and metal detector requirements (early 1970s), it had little expertise in human factors. Moreover, these technologies were relatively simple compared with aircraft cockpit and ATC consoles that the FAA had to certify without objective human-factors criteria, making human-factors standards for security a relatively low priority. However, many behavioral experts argue that properly developed human-factors standards could improve system performance for aviation security as well as safety.

In recent years, the FAA has issued regulations for security technologies-computer-controlled access at airports and explosive detection systems—that are considerably more complex and have wider system implications than x rays and metal detectors. **As has been commonly the case whenever new technology is used to solve a problem, attention is focused on the positive aspects of the technology—how effective it is—without giving full consideration to possible new human-factors problems caused by the technology. The lack** of attention to man/machine human-factors and system operating issues is evidenced in the explosive detection system (EDS) regulations published in September 1989[26] and the subsequent performance of TNA, the only device to date that could meet the FAA standards. Beyond setting detection criteria, which are critical to the security system performance, the FAA also included requirements for throughput of the device (which is primarily an economics issue—see ch. 4) and a requirement for 100-percent automated detection decisionmaking. Several lines of reasoning could lead to a design goal of total automation, including lower operating costs over the long run

Box 5-A—UAL Hi-Tech Screening

United Airlines is focusing on management practices in its program, called Hi-Tech Screening, to improve the quality of pre-departure screening and the public perception of this highly visible function. Begun in 1987 at Chicago O'Hare and San Francisco Airports, the program incorporated many of the selection and incentive steps later recommended in the ATA proposal, and also attempted to integrate technology and people by reconfiguring the screening environment to make it more pleasant for screeners and passengers as well as to improve operations. Although wages are still low, successful workers have the opportunity to join the UAL organization, instead of working as contract security personnel. Improvements include direct communication links to supervisors for oversight and advice to screeners, layout designed to minimize passenger delays, and multiple cues to passengers that security measures are being taken in a professional reamer (security supervisor in an elevated booth, passengers see themselves on video monitors as they go through metal detectors, signs describing procedures are clear and concise). United believes that the program has been successful to date in increasing public awareness and employee morale and competence. At Chicago, the employee attrition rate dropped by half and weapon detections and FAA test scores increased significantly (79 percent detection rate on FAA weapons tests prior to Hi-Tech and 92 percent subsequently). United has also installed Hi-Tech Screening systems in Denver, Los Angeles, Seattle, and Washington Dunes, with plans for additional implementation in the future.

SOURCE: Site visit to O'Hare, April 1990, and Richard Davis, Operational Security, United Airlines, Jan. 3,1991.

[25]For example, x-ray systems used primarily for carry-on baggage must meet the standards set by the Food and Drug Administration.

[26]54 *Federal Register* 36938 (Sept. 5, 1989).

and possibly removing human error from the operating loop. However, it maybe useful, and sometimes vital, to keep the human in the operating/decision-making loop, especially if he or she must respond during emergency or unusual conditions. As has been shown so far in TNA tests, the false alarm rate is well above earlier goals and human intervention is required quite often. While automation, in the context of an EDS, is a useful tool, and total automation may be an understandable goal, **requiring 100 percent automated functions in an EDS is not justified at this time. The** EDS regulations provide an example of where input from a group such as the FAA's Human Factors Coordinating Committee could help flag potentially troublesome human-factors aspects of security regulations.

Passenger Profiling

In-depth questioning of all airline passengers and detailed examination of each of their personal belongings and baggage is impossible in a modern transportation system. Since most of the millions of passengers that fly on U.S. airlines each year pose no security risk, targeting security resources on the small number of passengers who exhibit some elements of the threat "profile" is one way to increase security without clogging transportation flows. profiling can be a valuable component of a transportation security system, providing an independent complement to hardware-based (and often more expensive) explosives and weapons detection technologies. Successful profiling depends on a large support system including comprehensive intelligence networks and threat analyses, information system technology to process large databases, behavioral research and analysis, and trained and motivated screening personnel.

There are two general approaches to operational profiling. One compares passenger demographic and other background data (age, sex, nationality, travel itinerary, etc.) to historic or recent intelligence-derived "threat profiles." The other is based on the examiner's psychological assessment of the passenger, taking into account nervousness, hostility, or other suspicious characteristics. Most profiling systems currently use elements of both approaches to varying degrees.

Airline passenger profiling, in most cases, must be fast (and consequently cursory) enough so as not to impose excessive delays. In other security contexts, such as screening for the "insider threat" profile within an organization where time is not so critical, much more detailed background data and questioning is possible. A different, although overlapping, form of profiling is used by law enforcement and investigatory agencies. Given pertinent data and evidence from a crime scene or threat, experts compile a profile of likely social, psychological, and physical characteristics of the criminal. However, much of the work and methodology could be transferred from one of the broad profiling regimes to the other.

FAA Requirements for Profiling-Under Federal regulations, U.S. airlines must apply a relatively simple form of passenger profiling for international flights (e.g., questions regarding electronic devices), although airlines are not prohibited by FAA/DOT from conducting any form of profiling at any time. Whether or not a passenger is selected for closer scrutiny, such as a manual baggage search, depends on where his passport was issued (a factor that varies based on threat intelligence) and on responses to a series of questions aimed at identifying potential terrorist "dupes." Additionally, airlines must conduct random baggage inspections on a small percentage of otherwise unselected passengers for each flight. These requirements do not apply to domestic flights or to foreign airlines, which results in an obvious gap in protection for Americans. **The fact that foreign airlines that compete with U.S. airlines on international routes do not have to satisfy these requirements imposes an economic penalty on domestic carriers and weakens their ability to compete successfully with foreign carriers, which, in addition, are usually state-subsidized. Domestic airlines complain, with justification, that a "level playing field" should be established to avoid this unfair disadvantage. An option would be to compensate** U.S. airlines for the additional costs, either from Federal subsidies or from the Airport Trust Fund.[27] Alternatively, foreign carriers could be required to apply similar security measures on flights landing in the United States to those demanded of U.S. carriers. The United States has forced better security practices in foreign

[27] In 1976, Congress established a precedent for compensating U.S. air carriers for security measures incurred in international operations by authorizing nearly $10 million for fiscal years 1976-78 (Public Law 94-353, sec. 24). In 1982, Congress extended the authorized limit to $15 million (Public Law 97-248, sec. 524(d). Nearly this much was actually disbursed to four U.S. carriers.

airports by threatening **revocation of landing rights of carriers from those countries in the absence of improvements.**

U.S. airlines operating on European routes have been permitted to substitute their own profiling programs for FAA requirements.[28] Most U.S. airlines and many foreign carriers conduct more extensive profile screening than minimum FAA requirements at foreign airports and some U.S. international gateways. Some airlines train their international employees in profiling techniques while others hire contractors to handle security for their international flights. Proprietary profiling procedures used by these airlines are modeled generally on the Israeli El Al method of profiling which is more comprehensive (and intrusive) than FAA requirements and reportedly includes psychological, social, and political factors. Complaints by certain groups, such as Arab-Americans, claiming harassment, stem from carrier-initiated profiling, not Federal requirements.[29]

During the past 5 years, the FAA has developed and tested a computer-based profiling tool aimed at potential terrorist hijackers and saboteurs. The Comprehensive Passenger Screening Profile (CPSP) is both a checklist and decision aid for field officers and a data collection system to support profiling enhancements. It encompasses the current FAA required profiling procedures plus additional factors based on a data profile of terrorists, using historical and intelligence sources.

The decision process for selecting a passenger for further examination is automated through a series of mathematically weighted yes/no questions (some of which do not require passenger interviews), that the security officer responds to via a keyboard. CPSP is designed for easy modication if intelligence or data analysis indicates a need. In early 1990, the FAA offered CPSP as an option for airlines to meet profiling requirements. Continental Airlines and United Airlines have tested versions of CPSP at a few locations, and have been generally pleased with its performance, especially as a tool for centrally coordinating security management decisions and for providing a conduit for a detailed database.[30]

The FAA is considering making CPSP mandatory, but a number of carriers oppose it, citing security officer vigilance problems caused by distraction by computer keyboard and display. Knowledgeable FAA and airline personnel claim that airline opposition stems mainly from the increased oversight capabilities that such a system would give the FAA CPSP would provide a detailed record of all airline profiling actions (and errors or failures) that could be used for civil penalty proceedings. Presently, the FAA oversees airline profiling procedures through random or scheduled field visits.

The FAA counters that if a would-be malefactor sneaks through, CPSP also can provide documented proof that the airline followed FAA-required procedures, shifting some liability for a profiling failure to the FAA.[31] **Additionally, there is substantial analytic value to the large data set that would come from CPSP.** As discovered during TNA testing, little is known about the baseline average passenger and baggage; therefore, general background data, regardless of how well CPSP works operationally, would be valuable for security planning. No names of passengers are (or legally can be) included in such a data set maintained by the Federal Government.[32] However, as private entities, airlines can and do maintain such lists.

Other Issues for Human Factors and Profiling

Research and Development

Due to security and proprietary concerns, profiling systems in place today are shrouded in secrecy. The technical aspects of their development and quantitative measures of their performance are difficult to obtain, although the widespread use at airports across the world attest to airline confidence in profiling Given industry acceptance of profiling technology, the unregulated environment in which profiling systems were developed, and the potential enhanced capabilities and future needs, there is a

[28] Leo Boivin, FAA Intelligence, personal communication Oct. 18, 1990.

[29] Ibid.

[30] John Beardslee, Director, Corporate Security, Continental Airlines, personal communication, Oct. 15, 1990 and Glen Winn, Director, Operational Security, United Airlines, personal communication, Oct. 16, 1990.

[31] Op. cit., footnote 27.

[32] Ibid.

role for a concerted Federal (DOT) effort in profiling R&D.

The primary research fields of interest are in the behavioral sciences and in large database collection and analysis. A useful but neglected approach would be to investigate the role of cultural differences in establishing profiles. Since patterns of behavior considered anomalous in one culture are normal in others, understanding cultural effects better could lead to more effective and, possibly, less discriminatory use of profiles.[33] Relevant behavioral research with applications for profiling is being conducted by a number of Federal agencies, although they generally do not coordinate these research efforts.

There is a need to coordinate research and experience in developing terrorist profiles among concerned agencies. Also, some work is going on to establish databases of past incidents and known terrorists in order to help develop profiles. The FAA conducts a modest profiling research effort that produced the CPSP and is analyzing profiling field tests. **However, this effort is housed in the intelligence section under the Assistant Administrator for Civil Aviation Security with no direct link to FAA's R&D division.**

Historically, the FAA pioneered the use of profiles in aviation in the late 1960s and early 1970s during the upsurge of hijackings to Cuba. A team of experts under the leadership of the FAA Office of Aviation Medicine was involved in the development of the initial profiles. Limited use of profiles was made during the early 1970s and again in 1980, when immigrants from the Mariel Boatlift began hijacking aircraft to Cuba. [Profiles were employed on a limited basis to help stem the wave of hijackings to Cuba by some "Marielitos".]

In the 1970s, the FAA also developed a profile for domestic use to identify persons who might be carrying explosives or incendiary devices in checked baggage. This "checked bag" profile included several objective elements and was intended for use by airline personnel at ticket counters. This profile was never applied rigorously, although some of its elements were automated by at least one U.S. air carrier.

Thus, the FAA has had substantial experience with developing and implementing profiles for use in aviation security. It has worked with in-house experts, with other agencies, and with behavioral scientists under contract. **There should be steps taken to guarantee that this institutional knowledge is not lost, due to needed secrecy or personnel turnover.**

There should also be an effort to bring together knowledge on profiling from the Intelligence Community, from the Federal Bureau of Investigation, from the Immigration and Naturalization Service, and from the FAA, so that all agencies may profitably pool their knowledge. One way of helping assure such interagency communication would be the institution of annual interagency conferences on the topic (see ch. 3).

Profiling techniques and related technologies are being added to current security R&D plans **at the** FAA Technical Center. The operational aspects of using automated profiling systems, such as data entry and human/computer interaction, are similar to those of many other technologies, and could benefit from further research and development.

A near-term research need is how best to combine profiling systems with the new security technologies now in the pipeline. In fact, arguments have been made that the TNA device can only function effectively when combined with profile-based selection of baggage to inspect, since false alarm rates are high. This is, in fact, being done at the Gatwick tests. Presently, the profiling process results in binary decisions—let the passenger pass into the normal security process (more than 95 percent of passengers) *or* conduct a manual search of the passenger and his baggage. **One possibility would be to expand and refine the decision outcome from profiling to provide multiple screening paths for passengers depending on the level of threat and the availability of advanced detection equipment (see ch. 4).**

A longer term research option is to investigate new technologies to enhance profiling. Rapid access in the field to Federal, international, and, possibly, private databases (i.e., hotel, credit card) could greatly enhance capabilities. Remote sensing of respiration and heart rates and other biological parameters, combined with large population databases, automated facial-recognition systems, and

[33] Customs officials in the Northern Mariana Islands, a U.S.-flag territory, incorporate cultural characteristics in looking for anomalies for profiling.

biometric passports, all offer new possibilities for on-the-spot psychological and physiological assessments.

Civil Liberties

Security systems in general, and profiling methods in particular, trade certain freedoms (e.g., privacy) for safety. profiling methods, based on specific individual characteristics, may be derived from historical experience (e.g., the large number of Cuban refugees who hijacked aircraft to Cuba in the early 1970s or the examples of hijacking engaged in by members of various Middle Eastern terrorist groups). These characteristics sometimes include physical and cultural features, since these traits are the easiest indicators to verify. Often such subjects belong to readily distinguishable minority groups. Therefore, people who possess the characteristics in question but who have no ill intentions (obviously, the great majority) could be subjected to scrutiny that could be considered to encroach on individual freedoms.

This study describes measures to meet compelling public safety interests. It is, however, beyond the scope of this study to discuss the many legal and societal civil liberties issues involved (e.g., how much intrusiveness on privacy is countenanced by a compelling interest of the state?). It is certain that the technical ability to investigate and record personal histories and characteristics and the demand for the use of such ability will greatly expand, thereby increasing the potential for crossing the fine line protecting constitutionally guaranteed individual liberties. Legislative attention will have to address the tradeoff between public safety and welfare and civil liberties.

Incident Management

Human factors also play a role in managing incidents abroad. When U.S. citizens are held hostage in a foreign country, the United States often plays a role in resolving the incident. Some foreign security officials are trained in the United States under assistance programs. But the United States also may participate actively, as it did in responding to a number of airline hijackings in the 1980s.

From past experience, cultural factors particular to the country where the event is taking place frequently influence decisionmaking by local authorities. Some observers report that U.S. officials who were involved would, on occasion, have benefited by a more detailed knowledge of the dynamics of local social systems. For example, in some cases, although crisis management officials were supposed to be in charge of handling an incident, local cultural or political factors have resulted in the crisis being directed instead by senior office holders, who are untrained for the purpose and unable to provide the rapid decisionmaking that is often required.

Some research into systematizing knowledge of relevant aspects of different social systems would be useful. In this area, as in profiling, the construction of appropriate databases would be of use to U.S. officials who may be called on to participate in resolving a crisis. At present, there appears to be little coordination among agencies in understanding behavioral aspects of incident management. This lack provides another argument for strengthening interagency coordination in counterterrorism (see ch. 3).

Policy Options

The following policy options address human factors and aviation security.

1. Enhance FAA attention to human factors in security:[34]
   - Explicitly address aviation security in agency-wide human-factors planning.

     The FAA has taken measures to move in this direction.
   - Bolster human-factors expertise under the Assistant Administrator for Civil Aviation Security and the Aviation Security Research and Development Service at the FAA Technical Center by adding professionals to their respective staffs, especially in light of plans to increase staff levels of both sections significantly during the next few years. One such professional has already been added.

[34] The following recommendation, included in earlier drafts of this report, has already been implemented by the FAA
• Add a designee of the Assistant Administrator for Civil Aviation Security to the FAA's Human Factors Coordinating Committee.

2. Consider conducting R&D on combining passenger profiling techniques with other security technologies.
3. Give consideration to methods for "leveling the playing field" when imposing requirements on U.S. carriers but not on competing foreign ones.
4. Give consideration to civil liberties issues stemming from Federal aviation security requirements.
5. Coordinate behavioral research into profiling and incident management being conducted in the Federal Government. Arrange periodic interagency conferences on related topics.

Appendixes

Appendix A
The FAA Aviation Security R&D Program

Introduction and History

The most applied, mission-specific, and largest research and development program in the area of counterterrorism technology, and certainly the one most in the public's eye, is the FAA Aviation Security R&D program, conducted by the FAA Technical Center in Atlantic City, NJ. This program has been the focus of considerable attention, being reviewed by the President's Commission,[1] the National Academy of Sciences,[2] and by the FAA itself.[3]

This program suffers from its placement within the overall structure of the FAA, as well as its connection to the FAA Aviation Security program. The Technical Center Director reports to the Executive Director for Systems Development (within the overall FAA organization), who reports directly to the Administrator. Within the Technical Center, the Aviation Security Branch, which conducted the program, was until recently[4] a part of the Airports Division in the Engineering and Development Service. Thus, it was three administrative levels removed from the Director of the Technical Center. Last year, in response to both external and internal criticisms, the Aviation Security R&D program was elevated to the service level. Prior to the above change, the branch was staffed by only 13 personnel. The Technical Center, and, consequently, the Aviation Security R&D program, still has no direct line relationship with the Assistant Administrator for Civil Aviation Security (CAS). Figure A-1 shows an organization chart for the FAA as of August 1990.

The FAA's research and development programs started in the early 1970s to provide means of countering the perceived hijacking threat, Early research and development work was primarily in the area of metal detectors, resulting in the successful suppression of this threat. The September 1975 bombing at LaGuardia Airport first focused attention on the problem of detecting explosives, which has been the central focus of the R&D program ever since. In 1976, the R&D budget of the branch was about $1.5 million. The first proposal to investigate the use of thermal neutron analysis (TNA) to detect explosives was originated by Westinghouse in 1977. Over the next decade, two primary research areas grew to the prototype-hardware stage: vapor detection by chemiluminescent detectors and fast chromatography, and the TNA program. In 1984, Thermedics, Inc., of Waltham, MA, a subsidiary of Thermo-Electron Corp., became the primary contractor for the development of the vapor detection system and in 1985, Science Applications International Corp. (SAIC) and Westinghouse were chosen to demonstrate the TNA concept (in 1987, the Westinghouse funding was terminated). In the eighties, the FAA's R&D budget grew from $7 million to over $9 million per year, augmented by the procurement of six prototype TNA units (monitored by the Technical Center but funded out of the Office of Civil Aviation Security). In fiscal year 1990, the R&D budget was over $16 million; the budget for fiscal year 1991 was about $30 million. It is a rapidly growing program in a period of retrenchment in Federal budgets. Table A-1 shows funding levels for FAA Aviation Security R&D.

The main area of emphasis of the FAA Aviation Security R&D program is explosives detection. This is still by far the dominant effort in the program. A second area of investigation that has been pursued over the past several years has been a systems analysis of the airport security problem. The analysis includes system components such as training, procedures, technologies, and controlling access to guard all the ways and physical paths that threats (e.g., hijackers, weapons, explosives) may take to the aircraft. This program has been conducted by the Sandia Laboratory of the Department of Energy (DOE) under contract from the FAA Technical Center. One new area of emphasis is aircraft hardening against explosives and another new field of effort involves the study of the application of human factors to aviation security.

In response to the several intense reviews and criticism (particularly by the Presidential Commission) of the overall R&D program, dramatic and rapid changes are currently being implemented in its staffing, organization, funding, and outlook. The comments made in this report are primarily aimed at the situation that existed until very recently; many of the identified problems are well on their way to being corrected. However, some other problems discussed

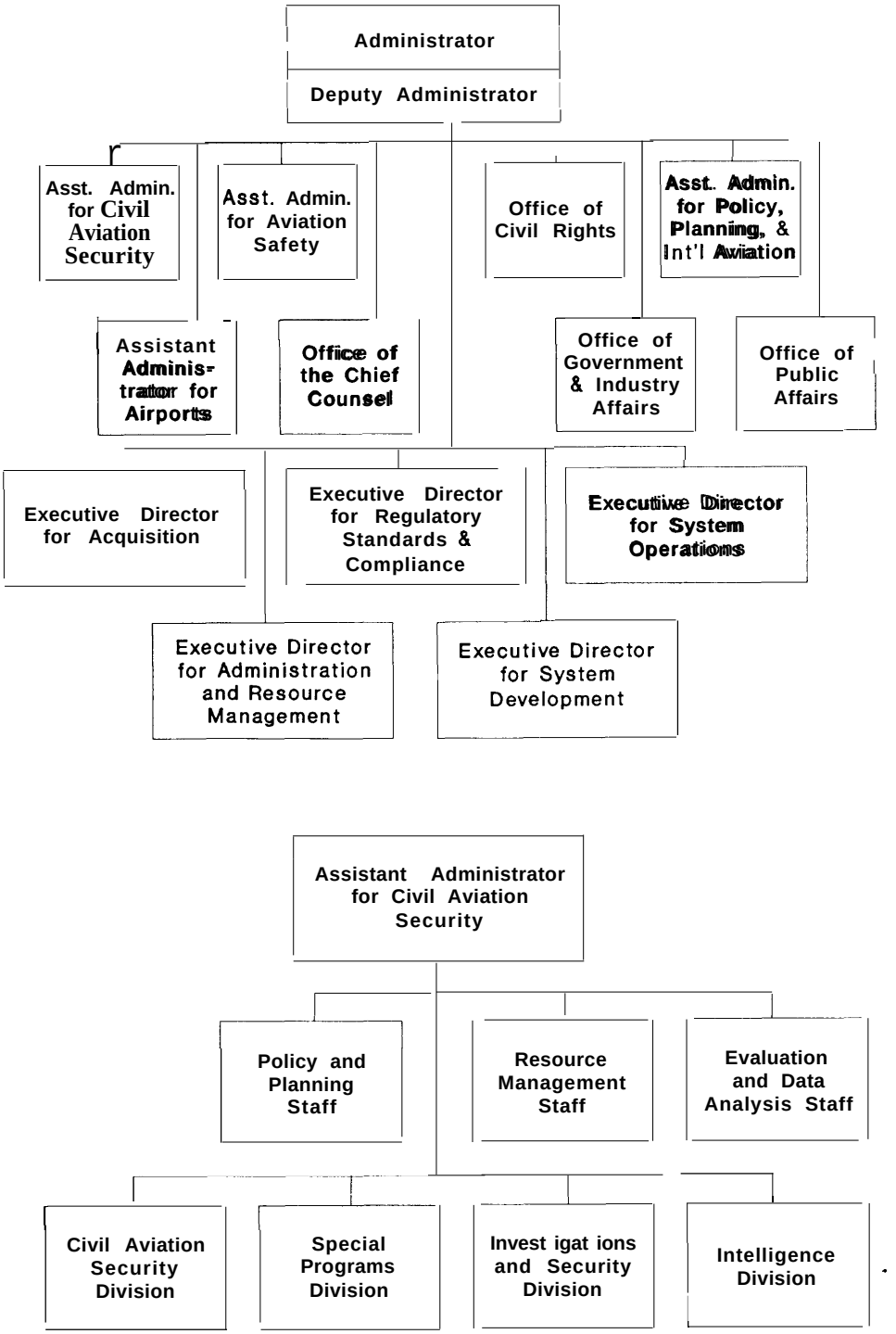
[1] The White *House, Report of the president's Commission on Aviation Security and Terrorism* (Washington, *DC:* May 15, 1990).

[2] Committee *on Aviation* Security, National Materials Advisory Board, National Research Council, "Reducing the Risk of Explosives on Commercial Aircraft," Publication NMAB-463 (Washington, DC: National Academy Press, 1990).

[3] U.S. Department of Transportation, Federal Aviation Administration, "Blueprint for Change: A New Security Organization," Report by the Office of the Deputy Associate Administrator for Appraisals, No. 90-2, Aug. 14, 1990.

[4] In response to the President's Commission on Aviation Security and Terrorism, the program was elevated to a "Service" level, the highest technical level in the Technical Center, reporting directly to the Center Director, and its staffing increased significantly (to 37 slots) as approved by the Administrator in July 1990.

Figure A-l—Organization of the FAA



SOURCE: U.S. Department of Transportation, Federal Aviation Administration, "Blueprint for Change: A New Security Organization," Report by the Office of the Deputy Associate Administrator for Appraisals, No. 90-2, Aug. 14, 1990, p. 3, figure 1a.

Table A-l—FAA R&D Funding Levels for Aviation Security

Fiscal year	Funding (in $ million)
1985	$7.4
1986	12.0
1987	14.4
1988	9.5
1989	9.9
1990	16.9
1991	30.3

SOURCE: Federal Aviation Administration, 1991.

hercin are still unsolved program and require further attention.

Current FAA Technical Center Research and Development Program

During fiscal year 1990, the FAA Technical Center security research and development program became involved in some controversial issues, notably the question of TNA testing and deployment, It has since undergone a complete reorganization and change of personnel. During these major diversions, the program has continued to function and is operating at ever higher funding levels, partially due to the infusion of new congressionally appropriated money, which was motivated by the report of the Presidential Commission.

The fiscal year 1990 program emphasized a continuation of research that had been ongoing since the previous year, with a few new starts made possible at the end of the year by the new money. A major innovation was the issuance of a Broad Agency Announcement (BAA) in November 1989,[5] a new way of inviting industry and academia to propose new ideas to the FAA for exploratory funding. The announcement specified the areas of FAA interest as follows:

- explosives detection-with a great deal of detail given about interest in various technologies of bulk and vapor detection of explosives,
- weapons detection,
- airport security,
- security systems integration, and
- aircraft hardening and blast/fragmentation containment.

During the year, the FAA received over 300 inquiries, over 80 white papers, and 68 actual proposals under this BAA. However, only five of these proposals were actually funded by the end of fiscal year 1990. Many of the industry groups that submitted formal proposals to the FAA under this BAA felt that the responses that they received were neither prompt not satisfactory. Of course, those that received no funding would naturally complain. However, a principal complaint was rather that no responses at all were provided for a long time. The apparent logjam in dealing with the BAA was likely due, in large measure, to the massive self-examination and reorganization that the FAA security program and the security part of the Technical Center were undergoing at the time.

In the bulk explosives detection area, the program was driven primarily by the conflict surrounding the SAIC/TNA. Testing programs were elaborated to allay criticisms of earlier tests of the system, TNA enhancements were funded to improve its performance, and, finally, other concepts were investigated, such as coupling TNA to other sensors to achieve better performance than achieved by the current XENIS (i.e., the TNA coupled to a conventional x-ray) system. A major program to develop a gamma ray resonance absorption explosives detection system under a joint program of Soreq Nuclear Center of the Israel Atomic Energy Commission and Los Alamos National Laboratory of the DOE was restarted. It had begun in 1987 as exploratory work, but had stalled when the program had matured into a more focused effort. However, the complexity of creating such a joint program delayed the start of actual new work on this program until well into fiscal year 1991. An upgraded program of research into the puked fast-neutron detection scheme was also initiated. Some new work was also started in NMR/NQR and on advanced x-ray systems, as well as on a positron emission spectroscopy scheme.

Another major funding area of the Technical Center has been the technology of vapor detection of explosives. A number of the past programs in this area were continued and several new ones started, including several basic technology investigations of the underlying science of vapor detection.

A third effort, the systems category, has been continuing. A major part of it, the integrated security system study at Baltimore/Washington International Airport, is moving from the conceptual stage to the hardware demonstration phase. A new program on aircraft hardening was also initiated under this element, initially looking at container hardening. This program element also includes the work at the National Academy of Sciences in support of the FAA program (both the overall evaluation resulting in the NAS report as well as support of the test program), Architectural and Engineering work on a new FAA explosives testing laboratory, and some miscellaneous expenditures.

The approximate program expenditures by element for fiscal year 1990 are listed in table A-2.

[5]U.S. Department of Transportation, Federal Aviation Administration, Technical Center, Aviation Security Branch, Broad Agency Announcement (BAA), TCBAA-90-001, ACD-120, November 1989.

Table A-2—Program Elements for Aviation Security R&D—Fiscal Year 1990 (figures in thousands of $)

Element T 1801A—TNA and other bulk explosives detection systems:	
TNA assessment support	$ 561
TNA enhancements	681
Other bulk detectors/dual sensor modifications	551
	$1,793
Element T 1801B-Vapor systems:	
Chemiluminescent detectors	$ 500
(Work at Sandia)	300
Mass spectrometers	1,065
Systems support	700
Research support	100
	$2,665
Element T 1801C—New technology:	
Gamma ray resonance absorption	$ 1,035
Pulsed fast neutron technology	1,300
Advanced x-ray technology	200
Biotechnological detection	257
Vapor systems research	1,233
Bulk technology R& D	1,080
National Academy of Sciences support	588
	$5,693
Element 1801C—Concourse access and miscellaneous:	
Millimeter wave technology	$ 465
BWI demonstration	3,000
Aircraft hardening	338
New laboratory-A&E study	500
Academic fellows program	200
Miscellaneous	600
	$5,103
Total	$15,254

SOURCE: Federal Aviation Administration, 1990.

Because of the FAA'S contracting procedures, in particular the late-in-the-fiscal-year commitments, much of the above work was scheduled to start in fiscal year 1991 and consequently could only be done in that year.

Current Problems

According to several studies, the FAA Aviation Security R&D **Service suffers from a number of difficulties. There are some technical problems, including a thin staff of experienced technical managers; a lack of systematic planning, particularly with respect to scope and requirements; problematic administrative support (insufficient number of contracting specialists) for timely contracting, and insufficient outside scientific advice and guidance. Further, there are a number of institutional problems, primarily due to the place of the Service in the** FAA **organizational hierarchy. There is a lack of coordination with the decisionmaking and operational groups in the FAA This R&D activity, in particular, requires strong coupling to the R&D work to the Civil Aviation Security operations groups. Some of these problems have been discussed in the report of the Presidential Commission, some in the National Academy of Sciences report, and some are enumerated in the FAA report on changing its security organization.**[6]

Critique by the President's Commission

The FAA has not met the challenge of developing effective detection technology to meet the progressively more sophisticated threat of terrorists.

> **The agency has not planned for the future but has reacted to past events. . . specifications were at best, of doubtful utility for terrorists have used plastic bombs at least since 1982 that are lighter than the weight specification for detection of plastic explosives by an EDS [explosives detection system] machine. . . today's TNA machines cannot, without an unacceptably high rate of positive false alarms, detect the amount of Semtex widely believed to have blown up Pan Am 103. . . . The TNA machine . . . although never scientifically tested, was approved by the Administrator of the FAA for use as meeting the specifications for detection of plastic explosives. . . without approval of the Technical Center that the TNA met the EDS standards. . . . The FAA needs to bridge the gap between what can destroy aircraft and what can be reliably detected. . . . Can steps be taken to modify airframes to minimize the damage? . . . The FAA for years did not have a continuing scientific and engineering advisory committee of independent, acknowledged experts to advise on its research programs. . . . The FAA must give higher priority and allocate more federal funds to R&D.**[7]

The commission made recommendations generally in line with these comments.

Critique by the National Academy of Sciences[8]

The National Academy of Sciences, National Materials Advisory Board, has probably performed the most detailed study of the FAA Aviation Security R&D program to date. A committee of 10 (primarily academic) experts with expertise in analytical instrumentation, forensic analysis, explosives chemistry, and nuclear sciences met 8 times between January 1989 and May 1990. The committee was briefed by the FAA officials and program managers and contractors, as well as by groups whose concepts were not currently funded. Committee members also visited specific laboratories to get briefings in more depth on some developments. A limited-attendance workshop was held to solicit new

[6] U.S. Department of Transportation, Federal Aviation Administration oP. cit., footnote 3.

[7] The White House, op. cit., footnote 1, pp. 63-66.

[8] Committee on Aviation Security, op. cit., footnote 2.

ideas from knowledgeable scientists with innovative concepts of how to attack the problem.

An important conclusion of the NAS study was that it is unlikely that any single technological means will significantly reduce our vulnerability to a sophisticated terrorist threat. Consequently it is clear that a succession of screening techniques or stages will be appropriate and explosives detection must be looked at from a systems or integrated point of view. Further, there are various costs involved in the implementation of any screening procedure: the direct costs of the equipment and the personnel required as well as the indirect costs of the delays or changed operational procedures that are demanded of the airlines. Consequently, any choice for security improvement is necessarily a compromise between the degree of security achieved and the costs imposed. This furnishes an argument for a well-thought-out systems approach to the specification of security requirements.

The National Research Council report came up with a specific set of nine recommendations and some program priority recommendations, which are summarized below:

a. Define a search strategy to optimize the mix of technologies that are available. No single detection technology is currently capable of providing the needed sensitivity and specificity required to provide security; a combination of currently available devices may well provide significantly better security than is now provided.
b. Implement low technology and human-factors-type improvements. Assure positive passenger/baggage matching on all aircraft, eliminate curbside luggage check-in, give specific consideration to passengers and baggage that disembark at intermediate stops, implement risk profiling of passengers, and bring about improvements in training, motivation, and monitoring of security personnel.
c. **Define performance criteria of detection systems. A minimum detectable-explosive quantity and a minimum vapor-detection sensitivity of 1 to 100x 10^{-15} gram was recommended. The quantity was in disagreement with the higher explosives quantities used currently by the FAA**
d. **Explore reinforcing aircraft baggage containers. Investigate the possibility of relatively simple inexpensive modifications that could increase the capability of the aircraft to withstand small explosions to the point where detection is made easier.**
e. **Establish standardized operational test procedures and testing facilities for explosives detection systems. A government operated (e.g., FAA) or supervised, yet completely neutral, test facility should be established to conduct standard tests and acceptance procedures on any detection hardware available. Field tests under realistic airport conditions were recommended.**
f. **In testing bulk or vapor explosives detectors, develop standard positive controls for routine checks of sensitivity of instruments and for blind checks of the system and observers.**
g. **Take advantage of systems integration opportunities for vapor detectors. Combine the best stages of various commercial instruments to create a more effective total system.**
h. **Explore the tagging of explosives and detonators to make them easily detectable. It has been suggested that the addition of small amounts of materials added to explosives and detonators could make them easily observable by inexpensive means.**[9]
i. **Continue the support of the exploration and the development of new methods that maybe applicable to explosives detection. The committee could not identify any approaches that were neither monitored nor funded by the FAA and recommended that the FAA continue its R&D program to keep abreast of the state of the art. This constituted an endorsement of a good part of the FAA R&D program.**
J. **Program priorities:**
   - **Establish an explosives detection systems analysis and architecture group.**
   - **Demonstrate passenger/luggage correlation schemes.**
   - **Solicit and fund proposals for aircraft hardening analysis.**
   - **Establish an operational testing facility.**
   - **Solicit and fund proposals for developing positive controls for bulk and vapor phase systems.**
   - **Select a prime contractor or systems architect to optimize vapor phase systems.**
   - **Solicit and fund proposals to demonstrate explosives tagging schemes.**
   - **Solicit and fund exploratory research proposals for new methods of explosive detection.**
k. **Funding recommendations:**

Major funding areas
- **airport-based nuclear accelerator**
  - **improved x-ray explosives detection**
  - **nuclear resonance absorption (NRA)**
- thermal **neutron activation (TNA)**
  - **x-ray computerized tomography (CT)**
  - **x-ray methods for bomb detection**

[9]OTA disagrees with this recommendation, as regards explosives: see 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), p. 51. OTA concluded that this proposal ignores the problem of the large amounts of plastic explosives currently available to terrorists as well as the fact tbat some plastic explosives can be manufactured by terrorist groups or can be obtained from state sponsors.

Moderate funding areas
- **chemiluninescent vapor detection systems**
- **fast-neutron activation associated particle**
- **glow discharge ionization tandem mass spectrometer system**
- **ion mobility vapor phase system**
- **nuclear quadruple resonance (NQR)**
- **pulsed fast-neutron activation (PFNA)**

Modest funding areas
- **fast-neutron activation (FNA)**
- **nuclear magnetic resonance (NMR)**
- **vapor phase component technologies**

Critique by the FAA Report[10]

"The office of Civil Aviation Security (CAS) has not provided adequate direction and oversight in defining and documenting adequate research requirements and has not set program priorities. . . . The Center currently works under a 1986 memorandum for explosive detector requirements. . . . There is no current comprehensive security R&D plan which delineates requirements for R&D projects and lists goals. . . . Communications between the CAS and the Technology Center have not been adequate. . . . There has not been continuous dialogue between CAS and the Technology Center. . . . The security R&D program does not contain the same operational test and evaluation or independent test and evaluation procedures that other agency R&D programs currently use to evaluate new technologies . . . the program has focused narrowly on technological solutions rather than thinking of aviation security as a system. "

OTA Comments on Concentration and Priorities

***In* any R&D program, concentration and priorities are a matter of judgment. However, several of the previously cited critiques point out, and OTA concurs, that the technical center program has been too narrowly focused, decoupled from the real world with respect to requirements, and devoid of an overall plan with goals and schedules.**

As an example of the narrow focus, the vapor detection program, although doing excellent work in this detection technology, focused on the concept of a personnel inspection booth using vapor detection equipment. The program should have asked the broader question: what is the basic capability of the equipment and how could such equipment be utilized in an aviation security system? Vapor detection capabilities are very scenario-dependent; the same equipment that may function well in one particular use may be useless in another mode.

There is strong evidence that some vapor detectors are able to detect plastic explosives. This case has been made by the Department of State as well as by several foreign governments and appears to be confirmed by some recent FAA tests. The issue is to devise a viable scenario for applying this ability to the aviation security problem. Several tests have recently been run to determine the capability of commercial vapor detection equipment in searching for explosives in electronic equipment as identified from x-ray images.[11]

A similar criticism applies to the FAA approach with respect to their evaluation of the SAIC/TNA. The TNA was pursued as an all-encompassing first and final inspection system. When its performance fell short for that application, both at the higher explosives quantities set by the FAA and at the lower value widely believed more appropriate, the FAA looked for supplemental measurements that could be used to fix its shortcomings. A more effective approach would ask what functions TNA can perform; possibly it could function as the high-cost, low-throughput device at the end of a chain of other systems that only inspects a few questionable items left indeterminate after other screening. Such an approach would run counter to the FAA'S earlier attempt to implement TNA as its chosen EDS.[12]

The R&D program also needs to make a clear decision on to what level of development a concept should be taken: should the FAA take technology all the way to a fully developed commercial prototype (as it is doing in the case of the SAIC/TNA) or is it the FAA'S responsibility to demonstrate the feasibility of a technology and to certify that it has demonstrated requisite performance levels? This issue touches on the definition of requirements for instrumentation developed by the R&D program. For example, the inclusion of a probably unnecessary throughput requirement that makes R&D difficult and expensive (see ch. 4). For long-term projects (on the order of 3 years or more), the R&D program should spend its effort on demonstrating sufficient measurement accuracy to satisfy the FAA performance requirements for sensitivity and specificity at given threshold quantity levels (which may be kept classified to protect information on the vulnerability of a future security system). From there on, the vendors and the airline (or airport authority) could negotiate the specific technologies they wish to implement to meet the FAA specifications,

[10] U.S. Department of Transportation Federal Aviation Administration op. cit., footnote 3, ch. 1.

[11] The FAA recently conducted an assessment of four commercial vapor detection systems for checking carry-on baggage in combination with other sensors (x-ray screeners), with some encouraging results that have not been released to date. Further, the Massachusetts Port Authority at Logan Airport, Boston, recently also conducted a series of tests utilizing Thermedics equipment.

[12] See 54 Federal *Register 36938* (Sept. 5, 1989).

subject to operational testing of the commercial products for compliance.

A related question is the issue of how much help the FAA should give: a single source can achieve a favored commercial position through significant government support. In lieu of being able to afford multiple approaches, which would be the fairest and best procedure, it may be preferable for the FAA not to fund one competitor all the way to a production prototype, but rather to restrict Federal funding to demonstrating the required measurement ability. The FAA should insist on proper and timely documentation of the results and the distribution of data gathered under federally funded programs to all interested competitors to the degree legally permitted. **An exception to this strategy maybe in order in the case of an urgent need to field equipment as soon as possible, such as might have arisen during the Gulf War, because of an increased terrorist threat. In such cases, rapid funding to prototype of a single project would probably be the most efficient path.**

The issue of a properly designed and implemented qualification test program for any and all detection systems was highlighted in the first OTA report.[13] As discussed in that report, the interpretation and use of test results was the root of much of the controversy for the SAIC/TNA. In particular, there was lack of agreement about the meaning of test results between the Technical Center and FAA officials responsible for regulations. The FAA Technical Center has taken a large number of constructive steps in the direction of developing proper protocols for such tests and for carrying them out.[14] The design and conduct of testing is another area where the utilization of a broadly based scientific advisory group, as recommended by several of the investigations, would be very constructive.

OTA Comments on R&D Program Requirements

The lack (or obsolescence) of realistic technical requirements for the Technical Center research program has been identified as a serious problem by several of the investigations. The setting of these requirements is an area where much better and closer cooperation is required between the Technical Center and the Assistant Administrator for Aviation Security. Inherent in the proper use of requirements to guide the research program is the need for the operational part of the organization to be in full agreement with these requirements, to coordinate with the Technical Center in their implementation and rulemaking process, and to be consistent in the interpretation of the test results regarding certification.

The issue of the proper mass of explosives that a detection system must be able to detect has been much discussed. Although it is true that some secrecy on the topic is a good idea, this does not obviate the need to set this requirement from a proper empirical and analytical base and to provide justification for the choice (even if the details are classified). There are ample data in various U.S. Government agencies, such as the FBI, as well as with foreign governments and agencies, to guide this choice. **FAA is currently collaborating with a number of agencies and with airframe manufacturers to derive a justifiable quantitative analysis of this problem.**

Aside from the primary issue of the weight of explosives to be used as the threshold, there is also some confusion about the type of explosives that should be specified. When a performance value is quoted for TNA testing, it is usually given as a weighted average of five commonly used explosives, including Semtex and TNT. Different threshold values are used for each explosive in an effort to account for the differences in the explosive power of the various products. Consequently, when a specific threshold is quoted, that value is an average and not necessarily applicable to all explosives.

One serious omission was propagated in this averaging process, with regard to testing the TNA system: the omission of a particular explosive that, in fact, has been a favorite of airline bombers for nearly 10 years. This omission has been redressed in recent independent tests at Gatwick.

A similar but less discussed issue is the FAA-specified requirement for throughput for a candidate detection system. This standard (currently set at 6 seconds per bag or 10 bags per minute for luggage checking) has been used in the past to decide that some concepts are not acceptable or are too Slow.[15] Though apparently straightforward, this standard is actually vague and performance with respect to this parameter is not well known, even for the much-tested SAIC/TNA. In fact, throughput performance is very application-specific. First, there has been no clear determination of the throughput requirement, which is location-specific—it can differ by over an order of magnitude between locations. The best work in this area is probably the recent report by the University of California at Berkeley done for the Air Transport

[13] U.S. Congress, Office of Technology Assessment, op. cit., footnote 9.

[14] The National Academy of Sciences has been asked to follow its previous study with a test protocol design for bulk detectors; Sandia Laboratories has conducted some studies of a test protocol; a group of four outside consultants setup a test protocol for and carried out a set of tests performed at Kennedy airport in April 1990 and at Gatwick in June 1991; Idaho National Engineering Laboratory has been tasked with developing protocols for testing vapor detectors and with carrying out some evaluations.

[15] See also discussion in ch. 4.

Association (ATA).[16] This work defines the required throughput in terms of bags per hour required to eliminate or minimize queuing of luggage to practical levels. However, to relate this work to a given machine presents further problems since the specific use must be defined.

This work also discusses the interpretation of the throughput of the TNA system. The current TNA machine has a belt speed of 30 feet per minute, which gives it the theoretical ability to pass 10 bags per minute, if they are spaced with 36 inches between bag center lines. In that sense it meets the FAA EDS specification. However, at this spacing, the three radiation trap doors that contain the radiation would not be able to close, and consequently the machine would present a radiation hazard (according to Bureau of Radiological Health standards). In order to allow the doors to close, the spacing between bag centers needs to be about 52 to 60 inches, slowing the maximum rate to 6 to 7 bags per minute. This is the real maximum rate that a stand-alone TNA system with an automatic decision algorithm and a mechanism that can handle and remove the rejected bags.

If the system is coupled to another sensor, such as in the XENIS option, the correlation time of the two observations can become another rate-determining step. 'Throughput" lacks a simple definition and depends almost entirely on the specific operational use. Consequently the use of throughput in a certification protocol is probably misguided; throughput should be a consideration for the user to choose so as to meet the FAA's (and its own) operational requirements at a given location in the most effective and economic manner.

There is no reason why a comparatively slow (e.g., 1 to 2 bags per minute) system, with a high confidence (detection probability) and a high specificity (low false alarm rate), could not be a very attractive system when used in combination with other devices. In fact, it is quite probable that in a chain of different detectors, such as is likely to be used in overall detection systems, a slow, high-cost, final-stage filter will find a niche.[17] The throughput should not be an FAA-specified parameter, particularly at the R&D stage, but rather should be machine-performance information that needs to be considered in the selection of the specific role in which a detector is utilized.

In the area of vapor detection systems, current requirements are equally soft. It is difficult to specify the minimum amount of explosives that a device should be able to detect and to account for first-order countermeasures (e.g., wrapping explosives to trap the vapor). Again, the throughput is entirely dependent on the application scenario. The setting of specifications and standards is also a problem for current x-ray systems, since being able to differentiate the density steps of a test wedge, the currently used standard, is not very meaningful when x-ray systems are employed to attempt to detect explosives.

Finally, the issue of automation as stated in the requirements for an EDS needs to be clarified. The FAA EDS specification calls for an "automated" system. However, automation should be utilized so as to minimize the use of the human operator, yet should retain for the final decision process the powerful ability of the human to discriminate between many unknown items. In currently proposed systems, there is an operator that performs the final clearance of the automatically rejected bags, either from a careful study of a high-resolution sensor (usually an x-ray image) or, in the last resort, by a hand search. This level of automation may serve the requirement of relieving the boredom of human operators, which is generally cited as the primary reason for automation, except for extremely low false alarm levels. Of course, FAA officials are aware of this. A precise definition is, however, required to clarify the use of the term "automation" in the certification process.

The FAA Technical Center is currently developing a program plan to address, among other things, the setting of realistic technical requirements for security hardware. As part of this plan, possible future threats, such as new explosives or incendiaries, will also be covered. This effort is intended to resolve many of the problems noted above.

OTA Comments on Technical and Administrative Support

The technical staff available to manage the FAA Aviation Security R&D program has been limited in numbers; however this problem is apparently well on its way to being corrected.[18] One area where the lack of technical staff was very evident was in the responses offered to the BAA respondents. OTA heard many complaints of lack of FAA response from contractors that had submitted inquiries, white papers, and proposals under this BAA. Five contracts were issued under this request, specifically for:

- testing a competing TNA system at GammaMetrics;
- vapor detection work at CPAD, Canada;
- aircraft container hardening work at Jaycor;
- automation of the AS&E Z-Scan system; and

[16] Geoffrey D. Gosling and Mark M. Hansen, "Practicability of Screening International Checked Baggage for U.S. Airlines," Institute of Transportation Studies, University of California at Berkeley, UCB-ITS-RR=90-14, July 1990.

[17] This topic is discussed in greater detail inch. 4.

[18] Under the reorganization of the program into a Technical Center Service, the number of personnel Wetted to the program has been increased from 13 to 37.

. SAIC work in vapor detection.

OTA draws several conclusions. First, five awards do not constitute a sufficient number to encourage innovation and diversity; second, at least two of these awards were for work that was proceeding at the companies at the time; work that was well known to and even desired by the FAA-therefore, these contracts were not really the "innovation" thrust of the BAA, which was aimed at producing new ideas and concepts;[19] third, not all respondents in such a request received notifications of the evaluation and disposition of their submittals in reasonable time-they should have; and finally, all respondents should be informed of the actions taken and contracts issued so that confidence is built up in the community that BAA requests are a worthwhile place for industry to present their new ideas. The staff time to prepare these responses is a good investment in future relations with sources of innovation.

It also appears that the contract administration support given to the research and development program at the Technical Center was not very effective. Research and development organizations have a very difficult time with contracts that start and stop on a yearly basis. When the release of most of a fiscal year's funds are delayed until the last few months of that year, as has repeatedly happened in this program, great difficulties face those groups that have continuous programs. It also appears that the FAA has frequently taken an inordinate length of time from decision to signed contract.

Outside Scientific Advice

Some of the previously cited reviews of the FAA R&D program have recommended that the program make greater use of outside experts for advice and guidance in scientific and other technical matters. Suggestions have ranged from direct involvement of outside consultants in the program management to scientific advisory committees to give the program greater validity and "clout." OTA agrees with both of these suggestions and believes that liberal use of outside ''experts' could be very beneficial to the program. FAA is moving in this direction, following the requirement of the Aviation Security Improvement Act of 1990, which mandated the establishment of a scientific advisory panel as a subcommittee of FAA's Research, Engineering, and Advisory Committee.[20]

The FAA Technical Center program has used several university personnel as expert consultants with considerable success. Expansion of this type of use is highly recommended. The FAA R&D program is very broadly based, utilizing a wide variety of technologies, from nuclear physics to sophisticated electronics, from state-of-the-art artificial intelligence to physical optics and spectroscopy. Each of these areas has many experts who could be very helpful in giving advice in their areas. It is very easy for a generalist program manager to be "snowed" in some specialty area and either miss some obvious error or be trapped into "re-inventing the wheel." Outside experts are usually familiar with the technical leaders in their area of knowledge. These people, even if not knowledgeable about the FAA program, could make significant contributions to progress of the FAA program by relating the program to current research. Liberal use of outside consultants can also be very effective in assisting evaluation of new programs.

Institutional Problems

A research and development program can only be useful to an organization if it is properly connected to the overall management of the organization and to the fulfillment of the organization's mission. In the case of R&D into aviation security technologies, institutional disconnect has been a major problem. Not only was the program conducted by a minor part of the FAA Technical Center (as noted, this has recently been changed) but it has been decoupled from the functions of the former Office of Civil Aviation Security, now the Assistant Administrator for Civil Aviation Security. The latter situation manifested itself in improper and outmoded requirements (e.g., the amount of explosives to be detected), a lack of overall planning, and a variety of inconsistent interpretations of data and results, often by personnel far removed from the technology programs. The presence of these problems has not allowed the R&D program to serve FAA management well in its decision processes.

As mentioned earlier in this appendix, the FAA Technical Center reports to the FAA Administrator through the Executive Director for Systems Development. The Assistant Administrator for Civil Aviation Security also reports to the Administrator. Such an arrangement can only work if great care is taken in assuring the coordination between all pertinent functions, and if specific agreements exist covering the jurisdiction of the various groups. This has not been the case in the past.

Several groups have been directly involved with various aspects of the R&D program and with the applications of the results and data of that program. The R&D program is primarily located at the Technical Center. However, human factors as used in screening or profiling of passengers, was the concern of the Intelligence Division within the Office of Civil Aviation

[19] This may have been due, in part, to a natural tendency on the part of the contractors to present modifications of ideas that were funded in the pint, rather tban to be very innovative.

[20] Aviation Security Improvement Act of 1990, Public Law 101-604, sec. 107.

Security. For years there was, within the Office of Civil Aviation Security, only one individual assigned to monitoring the R&D program. For the FAA in general, regulatory standards are produced under an Executive Director for Standards; however, for aviation security, this function was subsumed under the Office of Civil Aviation Security (now under the Assistant Administrator for Civil Aviation Security). Thus, this function was removed from both other standards-setting functions and from the FAA Technical Center's expertise. The issue of aircraft vulnerability or hardening was pursued by the Investigations and Security Division. The relations between that program and the Technical Center were not at all clear; the Technical Center has only recently asserted leadership in this area. It is not surprising that aircraft hardening and human-factors consideration did not enter the Technical Center R&D program planning until very recently.

The notoriety and public attention given to certain aspects of the R&D program by congressional hearings, the President's Commission, and the publicity in the aftermath of the Pan Am 103 tragedy have also created difficulties for the R&D program. The threat (via the FAA rulemaking process[21]) to require a new-technology explosives detection system at many airports created the potential of major business for a confused explosives detection equipment industry. Seeking guidance in order to plan the allocation of their resources, industry sought out interviews with all levels of the FAA and also with congressional members, both those directly involved with the FAA security issue and those who represented home districts. It was not uncommon to hear of visits to all levels of FAA management, right up to the Administrator, by contractors wishing to either sell or emphasize the virtue of their devices. This environment is not conducive to conducting a balanced R&D program.

The Technical Center's R&D program should be open and responsive to the needs of those responsible for planning and supervising aviation security operations. However, a R&D program should be conducted in an atmosphere of responsibility and understanding by the people who are actually doing the R&D. Personnel responsible for security operations should not also be responsible for the R&D. However, they should and must play an important role in the planning and setting of the desired requirements as well as priorities, with R&D decisions left to R&D management. As has been suggested by FAA officials, this could be accomplished by developing a memorandum of understanding (MOU) between the representatives of the Assistant Administrator for Civil Aviation Security and the Director of the Technical Center.[22] Such an MOU was signed by the Assistant Administrator and the Director of the Technical Center on March 19, 1991. This is a very positive step.

Ideally, in this coordination, the CAS representative should speak for all aspects of the security operation, including rulemaking and intelligence functions, and the Technical Center for all R&D, including human factors. Further, CAS should insure that the data and results obtained in the R&D program will be used only as agreed to and warranted by the R&D personnel. The Technical Center, in turn, should be responsive to the needs of the CAS in setting their research goals and requirements. Following the achievement of the MOU, a coordinating committee for security research and development should be formed to meet on a regular basis and provide the feedback and assurance that coordination is accomplished on a timely basis.

Certain aspects of the proposed new FAA organization are in accord with these suggestions. Under CAS, a R&D staff is suggested. This is the proper place to focus all the coordination functions within the CAS and for the primary interface with the Technical Center. The new organization of the Technical Center, with its elevation of the aviation security program to the highest operational level, should place the responsibility for coordination properly with the Director of the Aviation Security Research and Development Service.

The Future-Beyond Fiscal Year 1991

As a result of the attention showered on the FAA Security R&D program an opportunity to make significant progress has developed. There has been a major reorganization of the Technical Center aviation security R&D program and the organization has been elevated in status to the highest level. A new Director of the Service has been appointed and a radical change in technical and program management personnel has occurred.

It is not known to what degree past institutional problems have been resolved. There may still be questions concerning the relationship of the Assistant Administrator for Aviation Security with the Technical Center program. Will the Technical Center be allowed to run its own R&D program? How will the planning and requirements effort be coordinated with the operational side (CAS)? Most important, how will the technical results be protected from misinterpretation by the operational personnel charged with implementing the new technology through standards and rulemaking?

With a budget of $30 million for fiscal year 1991, a significant increase in effort (from $16 million in 1990) occurred. Many projects compete for these increased funds. Further, there is strong pressure to produce new

[21] See FAA rules FR 5436938 and 28985, dated Sept. 5, 1989, and July 10, 1989 respectively.
[22] Department of Transportation, Federal Aviation Administration, Op. Cit., footnote 3.

prototype detection systems that will provide answers to the airport security problem in a short time. This trend must be balanced against a carefully laid out program to provide the basic foundations of detection-technology.

There will be pressures to jump to demonstration prototypes of systems that are still in the research stage, resulting in large long-term commitments that may interfere with a more deliberately planned and balanced approach. The role of the FAA aviation security R&D program should be carefully assessed: is it desirable to bring completed prototypes to the field-testing phase, resulting in commercial advantages gained by groups that perform the development contracts, or should the role of the FAA be to demonstrate the ability of a given technology to make the measurements required for its purposes to the specificity and selectivity required, but leave the prototype development to the competitive market? The latter lends itself much better to a broad attack on a problem where there is no single, simple answer and where a group of technologies must be established that, in various combinations, can provide the needed increment in security. The former maybe favored if there is urgent need to deploy equipment as soon as possible.

OTA'S Comments on Specific Technologies

A number of detection technologies in the near-prototype stage are at the point where they should be able to make a contribution to improving security within the next 18 months. With the experience gained from four field units, the capabilities of the SAIC/TNA should be well understood and its optimum role could be determined. This role may not necessarily be as the primary detector that handles all the checked luggage. The Imatron Computerized Tomography X-Ray Scanner may find its niche in the coming year. A key need there is to determine the length of time required for the system to discriminate bombs, possibly when guided by simpler x-ray scanners. The x-ray technique for looking at bomb components may prove valuable, if its performance can be properly defined. Further, the role of pattern recognition in x-ray technologies should be further evaluated.

If there are competing TNA systems under commercial development, the companies should be encouraged to bring these systems to the test phase where their capabilities and performance can be assessed. The creation of a test facility and an independent testing group, complete with impartial and well accepted test protocols and standards, should be a priority. Standards for testing new bomb detection devices should include a large set of passenger baggage (probably obtained from airlines' unclaimed luggage), reflecting a diversity of locations and seasons. The approach to the testing and certification effort must be broadly based so **that** all types of detectors can be brought into this program and evaluated on an equal basis.

The development, or at least the evaluation, of the accelerator technology required by all the nuclear bulk detection methods, specifically for their use in public installations as required by the airport security program, should also be a prime objective. Without the requisite accelerator technology, most of the nuclear detector techniques will fall by the wayside due to practical considerations. The nuclear resonance absorption (NRA) concept is such a candidate: without a viable proton accelerator it is just an idea; with one, it may be a very competitive scheme. It appears premature to define a prototype for the NRA system at this time. An aggressive program to obtain the key answers to questions such as accelerator feasibility, detection threshold, detector scheme, and data requirement for discrimination, should lead to the knowledge base that is needed to define the optimum use of this technique. Such a sequential program will require considerable time, probably 3 years at least. An aggressive program directed at one of the other nuclear techniques (possibly pulsed fast neutrons or associated particle production) that measures both elemental and spatial distributions may also be promising. Which technique should best be pursued may well rest on the comparative ease with which the required accelerators can be developed.

Apart from detection devices, there are several areas that may bear fruit in the coming year. Increased attention to human assessment of the threat, the so-called profiling of travelers by skilled security personnel, is desirable. Positive passenger/luggage matching at the entry to the aircraft is another need. The role of the FAA Aviation Security R&D Service could be to bring the technologies together to develop an integrated system, since many of the technical pieces already exist commercially. It is a matter of giving the operators the best data and help so they can make the right compromises among cost, operational complexity, and effectiveness.

The work being conducted by the FAA Technical Center at the Baltimore/Washington International Airport, supported by Sandia National Laboratory, to implement a totally integrated airport security system is also of prime importance. This effort should operate with input from other groups, including FAA operations, airport operators, airlines, and those involved in the other technology R&D programs.

The final high-priority area for the future is aircraft hardening, discussed by both the President's Commission and the NAS study. In June 1990, the FAA Technical Center convened a meeting of government employees active in explosives and structural research and related topics to discuss and conceive such a program. This group developed and published a program plan that has served

the purpose of guiding this activity since that time.[23] Although it is a comprehensive and broad-based approach to the issue and recommends a combined analytical and empirical approach with frequent cross-checks, this report does not seem sufficiently technically based to provide the required guidance to the program. Since that report, more technically oriented efforts are taking place both within FAA and in cooperation with the Department of Defense.

[23]FAA Technical Center Plan, "Aviation Security Research and Development Plan for Aircraft Hardening," August 1990.

Appendix B
Explosives Detection: Dogs

This appendix and the following one will discuss two important areas of explosives detection that were only mentioned in passing in the previous OTA report on terrorism and technology.[1]

Introduction

The dog has been "man's best friend" since neolithic times, 10,000 years ago. As people learned to modify the dog's physical appearance and even its temperament through selective breeding, they were able to produce animals capable of performing a wide variety of services. These included refinements in the hunting process such as pointing, retrieving, tracking, and burrowing; herding; draft work (pulling and carrying); guard duties; providing companionship; and, more recently, assisting the disabled such as the blind or wheelchair-bound. Quite recently, police work has been added to the list.

In this last capacity, the dog has been making major contributions to the fight against terrorism, in no area more critically than in the search for hidden explosives. There is a lively debate between those who favor the dog as an explosives detector and those who place more faith in mechanical ''sniffers. " There are good arguments to support both sides. But to date, despite the best efforts of many talented scientists and technicians, there is no machine that is as widely used and accepted as the dog for the detection of explosives. This section will describe how and why the dog's nose has been applied to the task of detecting hidden explosives.

Disadvantages and Advantages

There are a number of disadvantages to using dogs as explosives detectors. First and foremost, adequately maintaining a canine operation, especially in the one-handler-to-one-dog mode preferred by many law enforcement organizations, is very expensive. Costs include initial acquisition of the animals, training for both the dog and the handler, veterinary and other maintenance expenses for the dogs, and the salary and other expenses associated with the handler, this last constituting the largest fraction by far.[2]

Explosives sniffer dogs do not and cannot operate by **themselves. They always function in tandem with their handler. The leash that connects man and dog is not so much a means of control as a channel for communication. This is both a strength and a weakness. When a team is in top form, the dog and his handler function with amazing** efficiency. But the dog works only as well as his master. Security searches are frequently boring, monotonous chores, the sort of task for which humans have trouble staying alert. If the dog senses a lack of commitment on the part of his human teammate, the dog's effort similarly diminishes. Also, it is inaccurate to say that the dog finds the explosive. It is up to the handler to recognize the sometimes subtle changes in the dog's behavior that signal interest in a faint scent. This reliance on the handler's judgment introduces a second opportunity for error.

Dogs have a number of weaknesses when compared to mechanical sniffer devices. Being a living creature, dogs cannot be worked as intensely as a piece of machinery. Depending on temperature and humidity conditions, a dog may be able to work only about 20 minutes before he needs a rest. Dogs are also vulnerable to distraction by loud noises, bright lights, new surroundings, fatigue, and alluring scents left behind by canine members of the opposite sex. Dogs have a limited attention span. They cannot be positioned beside a conveyor belt, even under comfortable conditions, and be expected to sniff luggage effectively hour after hour. They must be actively engaged in the search or their acuity will sharply diminish. They also are prone to personality quirks. Some dogs refuse to go in glass elevators. Some won't fly in helicopters. Some dogs bond very strongly to their handlers, some are more aloof. And it is the rare machine that produces the embarrassing "accidents" for which dogs are so infamous.

The dog also shares many of the shortcomings of the mechanical explosives sniffers. Because they rely on sensing airborne molecules or particles, dogs will not be able to detect an explosive that is perfectly wrapped. Also like machines, dogs can respond to the wrong thing. The U.S. Secret Service found that their dogs were reliably responding to the double stick tape regularly used to hold down small equipment in Air Force One. Perhaps a **cellulose nitrate was used in the adhesive. But this tendency to generate false alarms is apparently so unpredictable that the Irish Republican Army terrorists in the United Kingdom have been trying for years without success to devise a reliable masking odor for the bombs they plant.**

Probably the most serious liability of the canine approach is that it is largely unpredictable and essentially unquantified. How does the dog do his job? Is it just smell

[1]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).

[2]For some typical values, see the section of this appendix, below, in which the experiences of the U.S. Secret Service are discussed.

or are cues from other senses, such as vision or hearing, involved? Is it possible to tell, *before* **investing a lot of time and money, which puppies will make good sniffer dogs? These questions and others related to dog performance could probably be answered with some R&D effort.**

In the face of these disadvantages, why would anyone choose to use these animals? Basically, because they work. The primary advantage of using sniffer dogs over other methods of sweeping an area for explosives is that it has been shown to be effective. There is no mechanical device that is as accurate, fast, sensitive, mobile, flexible, and durable as a well-trained dog/handler team. Many organizations claim their dogs can even detect low-volatility explosives, such as TNT and the plastic explosives, RDX, PETN and Semtex.[3] No mechanical sniffer has been reliably shown to match this performance under field conditions. The dogs can go anywhere a human can go and can operate under any conditions tolerable to humans (although performance degrades with increasing temperature and humidity). They don't need electricity or batteries. They can be transported by helicopter, truck, car, or plane. They generally do not break. Service life is an average of 7 to 9 years. Thus, while they are expensive, they can be cost-effective for many uses. The dog/handler team operates in a real-time mode and thus can be much quicker than some sniffers that rely on sample collection followed by preconcentration and analysis steps. Also, the dog offers much more directional information than most mechanical sniffers and is usually better able to pinpoint the location of an explosive as opposed to merely alerting to its general presence.

Legally, a canine search is not considered invasive under the fourth amendment in distinction to methods that use any kind of penetrating radiation. Thus the searches can be conducted without a warrant. Finally, dogs are socially acceptable, at least in this culture. People are used to being sniffed by dogs and do not take offense or become fearful or belligerent.

It looks as if there probably will be a place for dogs in security work for the foreseeable future. But considerable progress has been made in the development of mechanical vapor detectors. Some people in the field estimate that within 10 years, possibly fewer, technology will be able to challenge or even surpass the detection capabilities of the dog.

Technology is also being applied to the animal systems in order to ameliorate some of the problems mentioned above. A number of organizations are considering efforts to **better understand the operation of the dog/handler team and to optimize it. These efforts will be discussed below.**

The Sense of Smell [4]

Of all the dog's senses, it is the sense of smell that is most renowned. Humans have made use of the dog's olfactory talents in a wide range of endeavors. Dogs now are used routinely to hunt for contraband such as drugs or weapons. They track escapees and other criminals. They locate earthquake victims buried in rubble. They assist in the investigation of suspected arson by searching for accelerants typically used by the criminal to start a fire. They even are used to find termites lurking in dark basements. Yet despite having used and relied on the dog's sense of smell for millennia, man still has little understanding of how this sense works.

Even in humans, much less in dogs, the sense of smell is not terribly well understood. It is known to be a chemical sense, requiring physical contact between the stimulant and the sensory organ. There are three pathways for reception of stimuli generally called odor or smell: receptor cells, pain endings of the trigeminal nerve, and, for some animals, the vomeronasal, or Jacobson's, organ. Anatomically, in dogs, as in humans, receptor cells are located high in the nasal cavity. The receptor cells are long and thin, terminating in about 6 to 12 olfactory cilia (delicate hair-like structures) that extend into the mucus layer that normally covers the inner lining of the nasal cavity. The other end of the receptor cell narrows to a fine nerve fiber and, joining with others of its kind, becomes the olfactory nerve which passes through the bony roof of the nasal cavity and then connects with the olfactory bulbs, stem-like projections under the front part of the brain. From there, additional complex neural connections are made to centers higher in the brain. Typically, there are millions of receptor cells in the olfactory mucosa patch, but for some animals, such as the dog or the rabbit for whom scent is very important, there can be tens of millions.

The second channel for sensory input, the pain or "free nerve' endings of the trigeminal nerve, are found throughout the nasal cavity and are also activated by many of the same stimuli that trigger the receptor cells. For example, these cells respond to orange oil, a relatively mild odorant, as well as scents more obviously irritating, such as ammonia.

The third channel is the vomeronasal organ, typically located in the hard palate of the mouth or the floor of the nasal cavity of some animals. It is believed to be

[3] See, for example, *Counter-Terrorism & Security Intelligence,* Bethesda, MD, Sept. 24, 1990, p. 6.

[4] The information in this section is from "Sensory Reception," *The New Encyclopedia Britannica,* vol. 27 (Chicago, IL: Encyclopedia Britannica Educational Corp., 1986) pp. 170-171; "Olfaction," *McGraw-Hill Encyclopedia of Science and Technology, 6th* **cd., vol. 12 (New York, NY:** McGraw-Hill, Inc., 1987) pp. 340-344; and Lawrence J. Meyers, "Dysosmia of the Dog in Clinical Veterinary Medicine," ***Progress in Veterinary Neurology,*** vol. 1, No. **2, 1990, pp. 171-179.**

important in detection of nonvolatile compounds and, for some species, pheromones. Its function in normal conscious scent sensation is not well understood.

In terrestrial mammals, the physiological steps involved in detecting odors can be broken down as follows:

- **airflow and sampling of odors,**
- **concentration of odors in mucus,**
- **odor-receptor molecular interaction,**
- **transduction, and**
- **. neural coding.**

While the receptor cells are located surprisingly far from the main airflow path (it is estimated that only 1 to 2 percent of the odor molecules inhaled during normal breathing actually reach the receptor sites)[5], apparently eddy currents carry just enough stimulus to the cells to cause arousal, whereupon sniffing will occur. Sniffing changes the airflow pattern and dramatically increases the number of molecules coming in contact with the nasal mucosa.

Odor molecules concentrate in the olfactory mucus on the order of 1 to 10,000 times their concentration in air. An apparently general olfactory binding protein in the mucus or in the ciliary membrane immersed in the mucus is involved with a reversible binding of the odor molecules to the receptors.

The exact manner in which the odor molecule and the receptor interact is another area that is not well understood. Mammals have a relatively small number of different kinds of receptors, estimated to be between 7 and 30, and each responds to a broad range of odorants. Yet thousands of different odors can be distinguished.

Once the odor molecule becomes attached to the receptor cell, the cell generates electrical signals to be sent to the brain in a process called transduction. Again, the mechanism by which this takes place and determination of the critical elements of the signal (pattern, repetition rate, signal strength, and so on) are areas in need of investigation.

Neural coding refers to the processing of the signals from the olfactory receptors in the various areas of the brain and is not well understood. Of all the senses, the pathways of the olfactory system through the central nervous system are uniquely complex. Some paths, apparently carrying strictly sensory information, link three different parts of the brain. Others are connected to structures of the limbic system, which are closely involved with control of emotions, feeding, and sex. This is consistent with observations of a strong influence of odors on behaviors and physiological regulation.

What makes something have a smell? Typically, the stimulant is a volatile organic molecule (only a handful of the chemical elements have odors although, obviously, some inorganic compounds such as ammonia and hydrogen sulfide (H_2S) are fragrant). To be detected by smell, the material must be volatile and, typically, the volatile organic compounds are soluble in water or fats. There are about half a million such compounds. Apparently, the nature of the perceived odor is influenced by both the shape of the molecule as well as the character of the chemical groups of which the molecule is made. Perception also varies depending on what other odorants are present.

The sense of smell in humans is said to be 10,000 times more sensitive than the sense of taste but sensitivity to odors varies from individual to individual and from compound to compound. For example, humans can detect 3-methoxy-3-isobutyl pyrazine (green bell pepper odor) at concentrations of about 1 part per 10^{12} parts of air, but methanol is far less easily detected and must be present as 1 part in 10^4 to be noticed. Temperature, humidity, age, respiratory infections, phase of the female hormonal cycles, and hunger all seem to affect sensitivity to odors. Among mammals, rats and dogs are credited with being the most sensitive to olfactory stimulation, one test showing dogs able to detect an odor at concentrations 10^3 to 10^5 times lower than humans.[6]

Continuing Investigations

Scientific work continues in an effort to better understand olfaction in general and the sense of smell in the dog in particular. Several years ago, animal studies were conducted at the University of Pennsylvania under support provided by the FAA, but were not followed up after the death of the researcher. Some work with rats has recently been reinitiated at the same laboratory, again under the aegis of the FAA. But the research is too embryonic to have yielded reportable findings yet.

Another group professes to be ready, willing, and able to perform serious study of olfaction in dogs but is having trouble securing funding. The Institute for Biological Detection Systems (IBDS) of Auburn University (Auburn, AL) was created in 1989. IBDS is made up of a team of scientists, veterinarians, and engineers whose aim is to improve existing methods of odor detection and to develop advanced sensing technology. They also would like to coordinate similar efforts at other institutions and corporations. They have received contracts and other support from private industry, foundations, the Department of Defense, and the FAA, but are interested in expanding their operation. In October 1990, they were expecting a memorandum of understanding from the

[5]D.A. Marshall et al., ''Olfactory Sensitivity to Alpha-Ionone in Humans and Dogs,' Chemical Senses, vol. 6, No. 1, 1981, pp. 53-61.
[6]Ibid.

Department of State, the U.S. Secret Service, and the FAA that would provide funding, but as of this writing, the Federal budget situation leaves this arrangement unconsummated.

This group has put a good deal of thought into developing a list of areas in which research should be performed and in developing preliminary outlines of experimental protocols to support such research. The range of questions these investigators would like to look into is an indication of the depth of human ignorance about this topic.

In response to an expression of interest by the U.S. Secret Service (although almost all security organizations relying on dogs expressed a similar need), IBDS considered means to investigate how to optimize the dog/handler team. They saw this effort as breaking down into several subsections. First, IBDS would like to devise a way to quantitatively and reliably evaluate the dog/handler team's detection capability. They would also like to improve the system for selecting dogs to be trained as sniffers and they want to establish means to evaluate and improve the training process. Finally, they want to explore possible ways to enhance the olfactory function of dogs.

In order to optimize the dog/handler team, the IBDS researchers want to start with an investigation of the sensory function of the dog. As an example of the means by which one may investigate the limits of a dog's sense of smell and the factors that affect these limits, IBDS proposed the following series of experiments. A test substance would be analyzed, using gas chromatography and mass spectrometxy, to determine the number and nature of its volatile constituents. Some preliminary work along these lines has recently been conducted by the Transportation Systems Center of the Department of Transportation. Explosives would be hidden in various detection "scenarios,' simulations of real-life situations, and the concentration ranges of the volatiles in the air surrounding the hidden samples would be measured. Then, the detection thresholds of dogs to each of the major volatile constituents would be gauged. This would involve selecting a fairly large group of dogs (at least 10) matched for such factors as age, sex, breed, and response to predetermined concentrations of baseline substances such as eugenol.[7] The detection threshold of the dogs to the test substances would be determined by olfactory methods (electroencephalography[8] [EEG] and behavioral olfactometry[9]) and by operant conditioning methods.[10] These procedures would be repeated under different conditions to determine the effect of variables likely to influence the dog's performance, including such factors as gender, temperature and humidity, circadian rhythms, and number, order, duration, and intensity of stimuli presentation.

Finally, the actual components detected by trained dogs would be determined by using a setup such as that shown in figure B-1. A sample of the test material would be injected into a gas chromatography (GC) where the volatile constituents would be separated. The passage of each separated component past the exit of the device is recorded as a peak on the chromatogram. A dog trained to respond to the test material would be positioned at a "sniff port" at the exit of the gas chromatography and the dog's response would be correlated to the various peaks. Because it is likely that dogs cue on a mixture of scents rather than on any single component, the IBDS team also proposes performing this experiment while exposing the dog to a blend of peaks from the GC.

Obviously, even this fairly limited endeavor is going to involve a lot of dogs, a lot of time and effort to train and support them, and, critically, a lot of money. In April 1990, IBDS estimated that it would need $480,000 to perform these tasks. Even if all these needs were met, there is some question about how reliably the results of such artificially constrained experiments could be translated to the field. But the desire for quantification of the dog's performance is very strong among the organizations that rely on them and was a repeatedly expressed need. Experiments such as these were recognized as a necessary first step in the process of understanding, and thereby optimizing, the performance of the complex biological system that is the dog.

IBDS would also like to be funded to explore optimization of the selection process and the training routine for both the dog and handler. For example, they would like to develop a battery of assessment procedures that would predict a dog's physical suitability (that is to say, freedom from disabilities), its trainability, and its performance after training. They propose a $100,000 project aimed at determining what factors (e g., olfactory capability, motor capability, intelligence, trainability, temperament, and medical/veterinary factors) and what tests for measuring these factors are most predictive of a dog's future success in explosives detection work.

For example, a panel of experts might be able to assess a dog's temperament based on a review of a videotape of

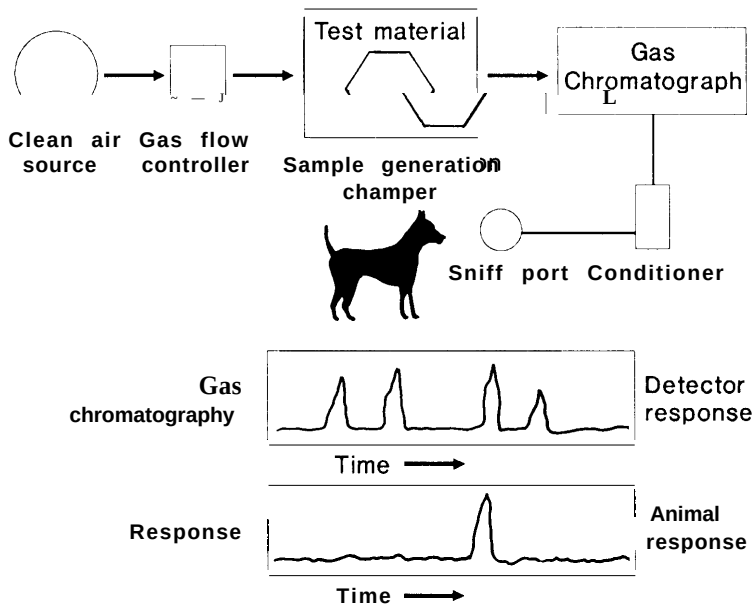
[7]The primary essential oil in clove oil.

[8]Electrodes attached to the animal's scalp record changes in electrical patterns in the brain in response to olfactory stimuli.

[9]Observation of an innate (perhaps reflexive) movement of the head towards or away from a stimulus red/Or sniffing or licking.

[10]The dog is trained to give a perceivable physical response upon detecting a sample. Then the concentration of the sample material would be lowered in stages until no response is given. This technique has the disadvantage of being extremely time consuming, taking about 8 weeks to adequately train a dog to give the proper response.

Figure B-I—Determining the Components of a Volatile Mixture to Which a Trained Dog Responds



SOURCE: Institute for Biological Detection Systems, Auburn University, April 1990.

an animal's behavior. Motor capabilities might be best evaluated by an analysis of gait and conformation, range of motion, or endurance tests. It is not easy to evaluate sensory capabilities in a nonverbal species. Some tests are based on detecting changes in electrical activity in the brain in response to sensory stimuli. Most tests rely on eliciting innate or reflexive behavior. Several means of assessing olfactory sensitivity already exist and may prove applicable. These include olfactory electroencephalograph and behavioral olfactometry that have already been mentioned.

Behavioral gustometry is a means of assessing taste acuity. Increasingly concentrated solutions of a taste compound are administered intravenously until a predictable response (usually a lick or a gag) is observed. This procedure can only be used to test sweet or bitter compounds because infusion of salty or acidic materials could adversely alter the dog's physiology.

Visual acuity can be assessed using the phenomenon of optokinetic nystagmus (OKN). In all species with moveable eyes, if the visual field is perceived to move, the eyes will follow the motion and then rapidly move back. To test **for visual acuity, the dog is presented with a moving grid pattern. The pattern is gradually made finer and finer. If OKN is observed, then it can be concluded that the animal can resolve the grid lines. At some point, the dog ceases to perceive a moving grid but sees only a constant grey** background and OKN stops. This threshold is an indication of visual acuity.

Behavioral audiometry is a technique for measuring the threshold for sound detection. The dog is exposed to sounds of various loudness and pitch and a reflexive response such as ear twitching or startle is noted. Unfortunately, this technique is not very good for **determining minimum threshold sensitivity because the animal does not reliably respond to noises that are detected but apparently not considered as needing further investigation. The IBDS team would like to investigate whether electroencephalograph might be a more suitable test.**

A separate proposed study would investigate the suitability of several new physical screening methods. In particular, a number of musculoskeletal abnormalities (e.g., hip dysplasia, common in German Shepherds) render a dog unusable. Yet this particular problem is not necessarily visible using conventional x rays until the animal is several years old or the disease well advanced. Work recently completed at the University of Illinois has demonstrated that the technique of gait analysis is effective in predicting the onset of hip dysplasia at age 2 in dogs 6 to 12 months old. This technique measures the relative amount of weight the dog places on each limb as he trots over a pressure sensitive plate. The IBDS researchers would like to investigate whether this technique should be included in the battery of physical

examinations conducted on dogs who are candidates for explosives detection work. They would also like to follow up on work done at the University of Pennsylvania using a new radiographic technique that measures hip joint laxity.[11] There maybe a correlation between this phenomenon and the later onset of musculoskeletal diseases thereby allowing for early diagnosis of such problems. Finally, there is some evidence that changes in bone metabolism could also be predictive of dysplasia. These changes in growth and resorption can be monitored by following the movement of a radioactive taggant and using a high-resolution tomographic imager. Auburn estimates that it would need about $120,000 to develop these physical screening procedures.

Another study proposed by the Auburn team would involve investigating training procedures for both the dogs and their handlers. To do this, they would perform a survey of existing detection training techniques for dogs, analyze which of those techniques are effective (which, of course, would require development of some measures of effectiveness), and develop improved training techniques based on these analyses. They expect that a number of factors might influence the success of a training program. These would include:

1. **the number and duration of daily training sessions,**
2. **the sequence in which "subtasks" are trained,**
3. **the optimal proficiency required on one "subtask" before training is begun on the next "subtask"**
4. **the type and schedule of reinforcement for correct performance,**
5. **the type of consequences delivered for incorrect performance, and**
6. **the role of the handler in detection tasks.[12]**

IBDS estimates that $400,000 would be needed for this study.

There are several other avenues for investigation proposed by the Auburn team. One of these involves a proposed $180,000 study exploring the influence of drugs on behavioral measures of olfactory function in order to try to find some agent that could enhance odor detection. There is some speculation that drugs could be used to alter:

1. **olfactory sensitivity,**
2. **odor discriminatory capacity (e.g., by increasing the signal-to-noise ratio),**
3. **olfactory memory,**
4. **attention mechanisms, or**
5. **motivation. 13**

Some preliminary work along this line was done by R. Doty at the University of Pennsylvania and the researchers at IBDS. Some of this work suggested that, in rats, low doses of amphetamines enhanced odor detection capability. Of course, this approach runs the risk of altering the behavior of the animal due to the intoxicating effects of the drugs. Other very preliminary research, for which the IBDS team would like $10,000 to run a pilot project, suggests that the sense of smell in the dog could be enhanced by ingestion of the target odorant.

This discussion of proposed projects came from a paper prepared by the Auburn group. It was designed to spark the interest of various governmental agencies that would have an interest in improving the explosives detection capabilities of dogs. Some of these projects may not be feasible, some may cost considerably more than estimated. However, IBDS was, at this writing, the only facility attempting to address the question of canine sensory capabilities in such a comprehensive, scientific way.

Other Avenues of Investigation

Several other groups are looking at novel ways to make use of animal olfaction to enhance security. A group in South Africa is marketing a system that it hopes will prove to be the best of both worlds. They use a mechanical device to collect and concentrate vapor samples. A vacuum source draws large quantities of air through cartridges containing an adsorbant material. In this manner, large volumes such as freight cars on trains, shipping containers, airmail pallets, airplane cargo holds, and so on can be sampled quickly and efficiently without unpacking. The saturated cartridges are then presented to a dog specially trained to detect odors from contraband. The manufacturers claim that this process works faster and better than normal dog operation. Objective evaluation of their claims is not presently available. Others have suggested that odorants easily detected by dogs should be used as taggants in explosives.

Animals other than dogs have been suggested for use. Some rodents, notably rats and gerbils have already been tested for this role with less than satisfactory results. Pigs apparently have an excellent sense of smell but their use by law enforcement agencies has been ruled out for aesthetic and practical reasons.

Finally, 10 to 15 years into the future, research into the "artificial nose" may pay off. Again at IBDS at Auburn University, researchers have taken small bits of natural membrane from olfactory receptor cells and fused them onto an artificial lipid substrate. When odorants bind onto

[11] The amount of mobility in a joint.

[12] A Discussion Document on Enhancement of the Dog-Handler Team and Development of Antibody-Based Sensors, ' submitted to the U.S. Secret Service, by the Institute for Biological Detection Systems, Auburn University, April 1990, p. 11.

[13] Ibid., p. 15.

receptor sites in the membrane, electrical impulses are given off. In the living creature, these would be transmitted to the brain, which would decode the signals and identify the odor. In the 'artificial nose' these signals are detected by sensitive electrodes and processed by a computer. The "nose" is very sensitive, responding to very low levels of odorant. But so far it is not very specific. "It cannot yet distinguish between different odors," says main researcher Vitaly Vodyanoy. Future research is aimed at improving selectivity. The researchers speculate that different odors may cause different electrical patterns to be produced. Alternatively, receptor cells may be differentially sensitive to different kinds of odorants.

The U.S. Secret Service Canine Explosives Detection Teams

Many organizations rely on dogs for part of their physical security routine. The Federal Aviation Administration, the U.S. Customs Service, all military services, the U.S. Park Police, the U.S. Capitol Police, many State and local law enforcement agencies, and numerous foreign organizations, such as the Royal Canadian Mounted Police, and the Royal Ulster Constabulary in Northern Ireland, use canine teams.[14] Since 1975, the U.S. Secret Service (USSS) has also trained and maintained a canine unit, the largest single canine bomb detection squad in the country. The background and operation of this organization are fairly typical and give a good insight into the pros and cons of using dogs.

The USSS is charged with protecting a long list of notables **including the President and Vice President, their families, visiting heads of state, and other dignitaries. They also provide security at the White House complex, other Presidential offices, and foreign diplomatic missions.[15] Part of this security involves searching structures, vehicles, and individuals for threats including explosive devices. For this task, the USSS employs dog/handler teams. It should be noted, however, that the USSS never relies on these teams as the sole means of explosives detection. They are always used as part of an overall Explosive Ordnance Demolition Unit and in conjunction with another search technique, either manual or mechanical, although the decision as to which search means is primary and which is backup depends on the situation. The dogs' place is as a tool for use by the security professionals.**

The USSS canine corps currently consists of about 30 dog/handler teams. Generally, these teams spend about 80 percent of their time doing detection work with the remainder spent performing patrol functions. It is uncommon, for cost and operational considerations, for any organization to dedicate dogs solely to detection work and so, frequently, the same animal is used for both detection and patrol duties. This cross use is not necessarily bad. The obedience training that is a necessary part of the patrol training process, improves the control and operation of the animal in the detection mode. The USSS dogs are trained to detect only explosives. They are not cross-trained to detect both explosives and narcotics (or other drugs). This is for safety reasons. If a dog were trained to give the same response to both types of contraband, the handler would never know which type of threat he was dealing with. If the dog were trained to give different responses, there still would be the lingering doubt about whether he was giving the proper signal. Because the courses of action following detection of these two types of contraband are drastically different and because the consequences of making the wrong response can be so dire, the USSS did not want to risk having their dogs give an improper alert.

Many breeds of dogs are probably suitable for detection work but patrol and guard dogs must be large and trainable to present credible attack behavior. For this reason, German Shepherds are frequently the breed of choice although several factors count against them. These include a difficulty getting physically sound dogs because careless breeding, especially in the United States, has resulted in the proliferation of animals genetically predisposed to physical disorders such as hip dysplasia. Also, German Shepherds, while controllable, are not as easy to work with as other breeds. Labrador Retrievers, for example, are less expensive, longer lived, more tractable, have good noses and (to date) no predisposition for debilitating diseases. However, their generally genial disposition renders them not particularly suitable for criminal apprehension[16] work Beagles, even poodles, have been considered for use as detection dogs but to date, no scientific comparison of the olfactory capabilities of various breeds has been undertaken.

The USSS is a great believer in the use of dogs and they are willing to pay quite a price for the privilege. Their expenses start with acquisition of the animals. The USSS relies on a breeder in the Netherlands who selects young (1- to 3-year-old) dogs, usually German Shepherds or

[14] This list is far from complete.

[15] The USSS is part of the U.S. Department of the Treasury and investigates many varied currency-related offenses such as forgery, violations of the FDIC Act, and those pertaining to electronic funds transfer frauds, credit and debit card frauds, false identification documents, computer access fraud, and misuse of U.S. Department of Agriculture food coupons. But these activities do not involve the use of dogs and so will not be further discussed.

[16] A euphemism for "attack."

Belgian Malanois.[17] The Service has found that this individual is their most reliable source of high-quality dogs. Because the dogs will also be used for patrol work the generally larger males are preferred. The dogs usually have had preliminary obedience and patrol training and cost about $2,000 apiece. Shipping adds another $400 to $500.

The handlers are selected **from the ranks of uniformed USSS** officers. They are chosen based **on an** evaluation of how well they work with the dogs and their general seniority in the ranks.[18] The only physical **requirement, beyond those normally associated with the Service, is the ability to pickup and carry 80 pounds, the average weight of a dog. Both men and women serve as handlers. The canine corps is considered desirable work among the USSS officers. At the very least, there is the free use of a car and the opportunity for improved income. Dog handlers are considered "technicians" which, by itself, justifies a pay raise of about 6 percent. In addition, considerable travel is inevitable, which translates into considerable overtime pay and, for care and feeding of the dogs, the handlers receive 2 hours of overtime pay every day for as long as their dogs are alive and working.**

Training is conducted at the USSS Canine Training Facility in Beltsville, MD. Small groups of new dogs and rookie handlers, typically four or five at a time, are trained as the need arises, about every 2 years. Deciding which dog to assign to which handler is more art than science. Some assessment of size (the larger dog goes to the larger handler) and home situation (the touchier dogs are not assigned to officers with small children) is made.

The USSS currently uses four dog trainers who are civilian employees of the USSS. Initial training lasts 20 to 26 weeks (40 hours per week) during which time, the teams are drilled in obedience, criminal apprehension, and detection techniques. For the obedience work, both on and off the leash, the dog is schooled to respond to the commands ''heel" (maintain a position at its handler's knee at any pace and through changes in direction), "stay' (remain in position even while the handler walks away or walks past), "down" (lie down on command, even if the handler is some distance away), and ''come" (return to the handler). To test and improve agility, the dogs are taught to cope with a variety of obstacles such as fences, windows, tunnels, broad jumps, ladders, and elevated cat walks.

Criminal apprehension training involves teaching the dog to chase and grab the arm of a suspect and to hold on until the handler arrives. On command, the dog must release the suspect and return to his handler. The dog then stands guard as the handler searches the suspect for weapons and will reengage if the suspect makes a threatening move. The dog must also obey a command to stop a chase, even if he is in full flight, and return to his handler.

For detection, the dogs are taught a three-step sequence: smell a target compound, alert, receive reward. To do this, the dogs are exposed to the scent of one of the target compounds, then the handler manually positions the dog into the "alert" posture, then the reward is provided. After an adequate number of repetitions, the dog comes to realize what is expected of him. The dogs must also be taught to follow the 'scent cone" to the site of the strongest odor. Training the handler to observe the environment and interpret the dog's behavior is critical here for the strength and location of the scent is strongly influenced by any air currents and eddies. The handler must be able to work the dog in a search pattern that takes best advantage of the air movements and he must be able to recognize when his dog is interested but not yet sure enough to alert. Commands are given verbally, with body signals (a wave of the arm, a sweep of the hand), or by using both modes simultaneously.

The USSS trains its dogs to signal detection of an explosive (alert) by sitting. Drug-detecting dogs are frequently trained to bite, scratch, and otherwise attack a suspect package. The passive "sit" response is clearly more appropriate when dealing with a potential hazard such as an explosive. The dogs learn to look for scents on the ground, in the air, and coming from objects, and they are trained to search for both humans (with the command "find him") or explosives ("search"). The dogs are trained to find about 13 of the most common military and civilian explosives including TNT, RDX, Semtex, and black powder. They do not train on peroxides which are considered too unstable to work with.

This seems like an impressive list of accomplishments. Yet, some dog-training experts estimate that a single dog can learn 150 tasks. A complex operation may involve a number of tasks but the USSS dog trainers believe that their dogs are asked to perform at a level of only about half their maximum capability.

Dogs require 70 to 130 iterations of a task before they can be considered trained in it. This time might be shorter for a very intelligent, talented animal or if the task is related to one already learned. For example, to learn to respond properly to the detection of a first explosive might take the full number of repetitions but to learn another explosive (where all that is required is to

[17] A breed developed in Europe during the early years of this century by crossing German Shepherds with hounds. The USSS finds them more suitable than German Shepherds because they have abetter 'nose,' they have abetter drive to work, especially in hot weather, their bite is about 100 psi stronger than a Shepherd, and they area little smaller and a lot faster.

[18] A minimurn of 5 years on the force is required.

recognize the new scent, the response procedures being already familiar) would be quicker.

Motivating the dogs is a supervisor's dream come true. The dogs generally will work to please their handlers who are lavish with praise when it is due. Furthermore, for criminal apprehension work, the dogs find biting the subject very rewarding in itself. Also, when they have performed successfully, the dogs are allowed to play with a ball. Usually this play is allowed to go on only for a few seconds before the handler removes the ball but it seems to satisfy the dog.[19] Food is used as a reward only as a last resort. The dogs are never punished for a false alert. They may not be rewarded if the handler feels the dog is "faking," but he won't be punished. False positives are tolerable, false negatives are not. The USSS does not want the dogs or their handlers to feel constrained about alerting.

At the conclusion of initial training, the dogs and their handlers are ready to join the canine patrol corps (although, as a practical matter, it may take an additional 6 to 18 months of experience before the dog and his handler become really comfortable working together). But formal training does not end at this point; in fact, it never ends. During regular working hours, the handlers repeatedly challenge their dogs by hiding ''training aids" scented with different explosive compounds. This not only gives the handlers a chance to test and hone their dogs' skills, but it also is very satisfying to the dogs, who, like people, can get very frustrated and bored if their work never seems to accomplish anything. All influencing factors are varied as much as possible. Therefore, the locale in which this training takes place, the kinds of explosives used, and the concentration of the explosive are randomly altered.

Additionally, on a weekly basis, every dog returns to the Beltsville facility for a full day (8 hours) of continuing training as part of a recertification process. During this time, he is tested against three or four explosives other than those used by the handler during the course of the week such that, over a span of a month or two, the trainers can be assured that the dog is still properly responding to the whole range of explosive threats. Should an animal fail recertification, it would return to Beltsville for additional training. This USSS recertification routine is much more stringent than that of many agencies. The FAA for example, recertifies their dogs only four times a year. Of course, the FAA generally uses their dogs for narcotics detection and if they should fail to perform correctly the consequences are not as immediately disastrous as a failure to detect an assassin's bomb.

The dogs go everywhere the USSS protectees go. The dogs are transported all over the country and, occasionally, all over the world. They ride like other animals, in travel kennels in the pressurized, but dark and noisy, baggage compartment. Despite this travel arrangement, most of the dogs seem to enjoy the excitement of being on the road and willingly enter their travel kennel. The dogs can suffer from jet lag, though, and several have washed out of the program from an inability to cope with travel.

An important feature of the USSS program is that the handlers have absolute authority to determine the fitness of their dogs for use on any given day. If the officer does not feel that the dog is performing properly, he or she can withdraw the animal from service without concern about being overruled by a supervisor.

Atypical day finds the dog and his handler reporting for the day shift (6 a.m. to 2 p.m.) at USSS headquarters in Washington, DC, where they receive their assignment. They might be sent to work 4 hours at the White House where the dog would be used to sniff a motorcade and then spend the next 4 hours on patrol around the embassies and other foreign missions.

The performance of the dog at explosives detection depends on several factors: the temperature, the humidity level, the amount of air movement, and, most critically, the skill of the handler in reading changes in the dog's behavior that signal a possible detection. As an example, for a search of a line of cars conducted outdoors, the handler would start the search downwind so that the dog would have the best chance to pickup odors. Handlers are issued small smoke generators to help them gauge wind direction. The animal is walked to the first car and given the command to search. The dog and the handler then circle the car. If the dog seems interested but does not alert (sit), the handler will note the behavior and continue the search, returning to the suspect spots later for a recheck. Ironically, newer cars are so tightly sealed around the doors, windows, and trunk that it can be hard for odors to seep out. Therefore special attention is paid to ventilation outlets and locks. Frequently, drivers are required to open the trunk to allow a closer inspection.

On cool, crisp days, the dogs can do sniffing work for an hour at a time, sometimes longer, before a break (on the order of 20 minutes duration) is needed. On hot, humid days, they may be able to work only about 20 minutes before they are exhausted. This behavior is quite the opposite of mechanical sniffers, which operate better under warmer conditions because more target molecules are evaporated and therefore are available for detection. Pavements are a particular problem. By catching and retaining the heat of the sun, the temperature around pavement level, where the dog's nose and feet have to do most of their work, can easily reach pain levels.

[19]Separating the dog from its orb is not always a trivial operation. Sometimes it is necessary to lift the dog by its collar until blood flow to the brain is choked off enough to cause partial unconsciousness before the dog can be persuaded to relinquish its grip.

Another distinction of the USSS program is that they dedicate one handler to one dog and the animals actually live with their handlers. Some organizations maintain a central kennel where the dogs are all housed communally. In some cases, there is not even any effort made to maintain a constant dog/handler team. Despite these apparent liabilities, some of these dogs still manage to work quite well. But given the mission of the USSS they cannot afford to have animals who are not well acclimated to humans in all their variations. They feel this is best accomplished by maintaining the dogs in a family environment complete with small children and other pets.

The bond between the team members seems to be a strong one. When the dog is retired from service, he is usually offered to his handler. Despite the necessity of signing mountains of paperwork acknowledging the risks of assuming ownership of a trained attack dog, most handlers choose to accept their teammates. One officer even delayed his own retirement in order to have it coincide with that of his dog so the two could stay together.

The average service life of the dogs is 7 to 9 years. Typically, when the dog retires, the handler also leaves the canine corps, either to retire himself or to assume other duties. The USSS generally has not recycled handlers through the program. This allows the maximum number of officers to participate, although some argue that this is a waste of a valuable resource, namely the trained handler.

In the end, has it been worth all the effort and expense? By maintaining the program, the USSS has clearly voted in the affirmative. But objective data is hard to come by. The problems of quantitatively assessing the dogs' performance have already been discussed and the USSS **is not immune to these problems. To date, the sniffer dogs have never found an explosive that would have actually threatened a protectee (apparently, they have not missed one either), although they have detected various weapons. No dog has been killed or wounded in action. Under training conditions, a detection rate of 75 percent is considered very good. A machine offering similar performance might not survive on the market. But finding plastic explosives 75 percent of the time is still a lot better than finding them none of the time. And as long as this performance level is acknowledged and the dogs are not relied on as the sole means of explosive detection, the Service is still ahead of the game.**

Furthermore, there is an undeniable deterrence factor in the use of dogs, especially in their guard and patrol functions The USSS feels this has inhibited the curious, and others with darker motivations, from trying to penetrate security boundaries.

Conclusion

As explosives detectors, dogs are about in the same boat as the FAA's thermal neutron analysis (TNA) device: they do not work very well, but they work better than anything else, at least so far. Again like TNA the competition is moving up fast.

There is some promise that research will enhance the dog's usefulness by: 1) improving our understanding of how the dog functions thereby making the dog's performance more predictable, and 2) by actually improving the dog's acuity. But research into mechanical sniffers is also proceeding apace. Devices capable of matching the dog's performance, at least in some respect, are nearly perfected.

Appendix C
Electromagnetic Detection of Metal and Weapons

Introduction

This appendix describes and assesses the potential of radiofrequency electromagnetic methods of detecting metal and weapons. The two major categories of methods are inductive methods, such as those used by metal detectors in airports, and reflectometry, including dielectrometry and short-range imaging radar.

Inductive Metal Detectors

Most metal detectors used at airports function either by detecting changes in mutual inductance caused by additional presence of metal in the portal or by detecting eddy currents produced in metal within the portal by a radiofrequency pulse. Those using the former technique are called mutual-inductance metal detectors (MIMD). Those using the latter, more modern technique are called eddy-current metal detectors; they can, in principle, acquire more information about metal objects and use it to improve specificity-i. e., discrimination of weapons from innocuous objects. Older systems used other techniques. All use the principle of electromagnetic induction and can be called inductive metal detectors.

Inductive metal detectors are likely to be useful for some time; however, they cannot detect nonmetallic weapons and, in order to reduce false alarms to an acceptable level, they require subjects being inspected to empty their pockets of metal objects. This slows inspection and precludes covert inspection. Designers polled by OTA believe there is some room for improvement in performance.

If a system is well sited to avoid electromagnetic interference (EMI), the signals of innocuous metal objects on searched persons may limit the performance of the system. However, if a system is poorly shielded or located near a strong source of EMI, the performance of the system may be reduced. In such a case, performance might be improved by better shielding or by relocating the system. If neither of these is practical, it is possible to improve performance by using a stronger magnetic signal to produce a stronger signal from metal objects-strong enough to be distinguished from the EMI.

However, the magnetic field to which the public may be exposed is limited to 1 gauss (1 G) by a standard (NILECJ-Std.-0601 .00) issued by the National Institute of Law Enforcement and Criminal Justice (now the National Institute of Justice) in June 1974 and by exposure **guidelines set by the Bureau of Radiological Health (BRH) of the Food and Drug Administration (FDA). The limit was set at 1 G because of concern that stronger fields might upset the operation of cardiac pacemakers. Some designers speculate that modern pacemakers are less susceptible to such EMI from metal detectors and that the maximum field could be increased without harmful effect. A committee of the American Society for Testing and Materials (ASTM) debated for several years a proposal to increase the limit to 3 gauss but has now abandoned pursuit of this aim, convinced that they cannot induce a disinterested third party, such as the National Institutes of Health, to do the human experimentation that would be required to prove safety at this level. They doubt that an ASTM standard, which would be characterized as an "industry standard," would be credible to all stakeholders.**

Some passengers wearing hearing aids have complained of the loud noise that an eddy-current metal detector can cause in some hearing aids, and some hearing aids have apparently been damaged by existing metal detectors. Allowing 3-G fields might exacerbate this problem.

Radio reflectometry is the measurement of radiofrequency electromagnetic (RFEM) waves reflected by an object. It is widely known that metal objects such as airplanes reflect radio waves that can be detected by radar receivers.[1] Smaller metal objects, including firearms, knives, and other weapons, can be detected at short range (a few meters) by low-power radar systems that maybe used to "frisk" suspects electronically. Because of concerns about health, x-ray or nuclear methods of inspection would be controversial or prohibited for this important application.

Simple, inexpensive systems can detect weapons but cannot generally distinguish them from innocuous objects. More expensive millimeter-wave (MMW) radar systems (so called because they use radio waves having wavelengths of a few millimeters) can display TV-like radar imagery of weapons concealed under clothing, permitting an operator to distinguish weapons from innocuous objects, reducing false alarms. Nonmetallic objects also reflect radio waves and can be detected and imaged by radio reflectometry. This is called dielectrometry; it maybe used to ''frisk' suspects electronically for nonmetallic weapons or explosives.

[1]Originally RADAR: an acronym for RAdio Detection And Ranging.

Dielectrometry

If an RFEM wave propagating through the air inside a suitcase encounters a material with a different refractive index, it will be partially reflected.[2] The refractive index of a medium is proportional to the square root of its dielectric constant (also called its relative permittivity) and to the square root of the magnetic permeability. Common nonmetals and nonferrous metals have nearly the same magnetic permeability as air, but in most cases, a different dielectric constant, so they will partially reflect an incident wave propagating through air. Estimating the dielectric constant of a reflecting material by irradiating it with radio waves and measuring the amplitude of the reflected wave is called dielectrometry. Some portable and relatively inexpensive dielectrometers designed to detect concealed explosives, weapons, and other contraband are already on the market. More sophisticated versions are in development.

SDA Model M600P, M600L, and M1800L Dielectrometers

Spatial Dynamics Applications, Inc. (SDA) of Acton, MA markets dielectrometers for use in detecting concealed items with a different dielectric constant than that of the material or space within which they are placed. One such device is the model M600P Portable Drug and Contraband Detector (see photo), which has been tested for operational effectiveness in detecting weapons (knives, firearms) concealed in various objects, and has been used to detect a concentrated solution of cocaine hydrochloride concealed in beer bottles. It is also capable of discriminating beverages from liquid explosives within bottles, and could thus play a role in many security applications, including airline security.

In response to a Broad Agency Announcement solicitation by the FAA (see app. A), SDA has proposed modifying the M1800L Laboratory Dielectric Tester to screen people for explosives or weapons. The modification would involve equipping the M1800L with an extended lens "suitable for screening people. " SDA also proposed designing an automatic scanning unit for the system. Extensive testing would be required to determine the device's capability and false alarm rate.

GDE Vehicular Detection System

The Electronics Division of General Dynamics Corp. (GDE) has developed and is marketing a Vehicular Detection System capable of detecting buried metallic objects, such as firearms (see figure C-1), as well as nonmetallic objects such as explosives, and displaying low-resolution images of them. This technology uses long-wavelength radar that is able to penetrate the ground to various depths (depending on the wavelength and power of the device and on the water content of the ground) and provide return images.

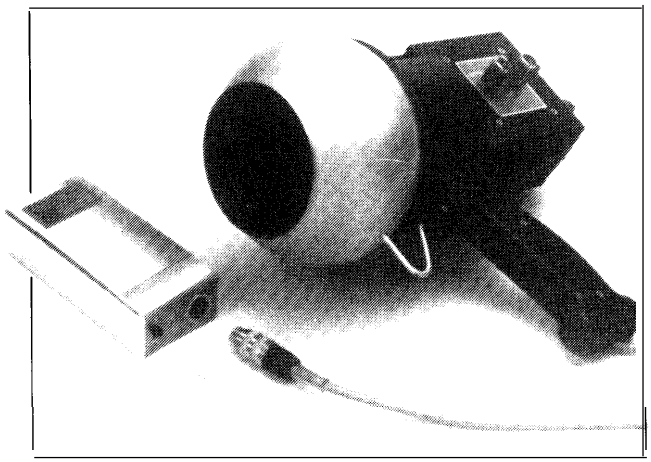


Photo credit: Spatial Dynamics Applications, Inc.

M600P **portable drug and contraband detector**

GDE Improved Hand-Held Detector

Under contract to the Defense Advanced Research Projects Agency, GDE is developing an improved, imaging version of a hand-held mine detector it expects to complete in 1991 (see figure C-2). The Improved Hand-Held Detector will be technologically similar to the GDE Vehicular Detection System.

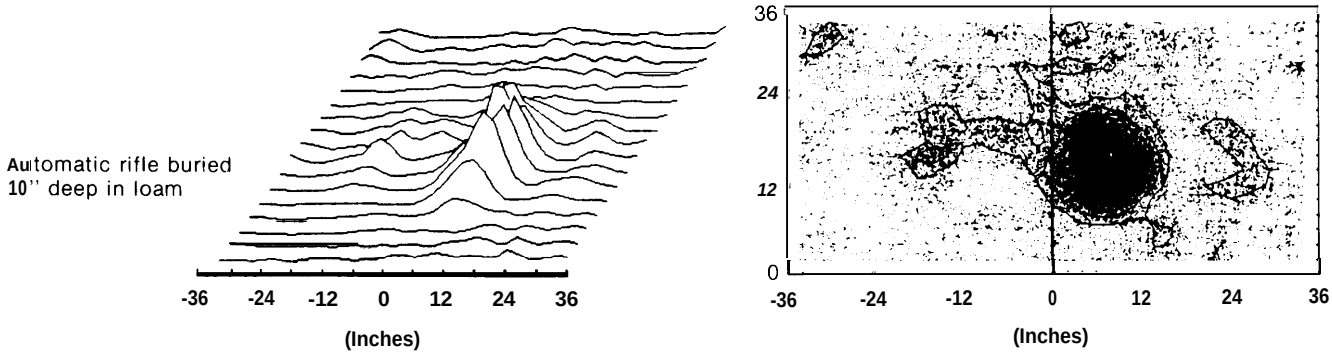
Millimeter-Wave Radar

Several short-range, high-resolution, imaging radar systems for detecting weapons concealed in clothing are now being developed. In weapons-detection applications, these compete with the commonplace mutual-inductance and eddy-curent metal detectors and with the existing and proposed reflectometers described above. Potential advantages of radar over such devices are: 1) radar images would allow weapons to be distinguished from coins, prostheses, etc., so the false-alarm rate would be low, and 2) suspects would not have to empty their pockets of innocuous metallic items; hence 3) suspects could be ''electronically frisked' covertly.

Distinguishing a pistol, for example, from a prosthesis requires imagery showing details as small as about 1 cm. Obtaining such resolution requires using waves with wavelengths shorter than about 1 cm—i.e., millimeter-wave radar.

[2] If the incident wave strikes the material broadside, the reflected electric field strength will equal the incident electric field strength multiplied by $(n' - n)/(n' + n)$, where n is the refractive index of the medium in which the incident and reflected waves propagate, and n' is the refractive index of the dissimilar medium encountered by the incident wave.

Figure C-l—Vehicular Detection System and Imagery of Buried Automatic Rifle



Signal strength plotted as height.

Dot-density plot with contours.

SOURCE: General Dynamics Corp., Electronics Division, 1990.

Figure C-2—Hand-Held Detector

This hand-held detector, under development by GDE, can detect buried, or similarly concealed, explosives. An improved version, to be completed in 1992, is being developed to produce imagery similar to that of GDE's technologically similar Vehicular Detection System.

SOURCE: General Dynamics Corp., Electronics Division, 1990.

The FAA **has funded competitive development of weapons-detecting MMW radars at two companies: Battelle Pacific Northwest Laboratories (PNL) and Science Applications International Corp. (SAIC). At present, the FAA is funding only the Battelle PNL work. Other companies developing millimeter-wave radar technology** applicable **to weapons** and explosives detection include Westinghouse (Advanced Technology Division, Baltimore), EVI, Inc. (Baltimore), and General Dynamics Corp.

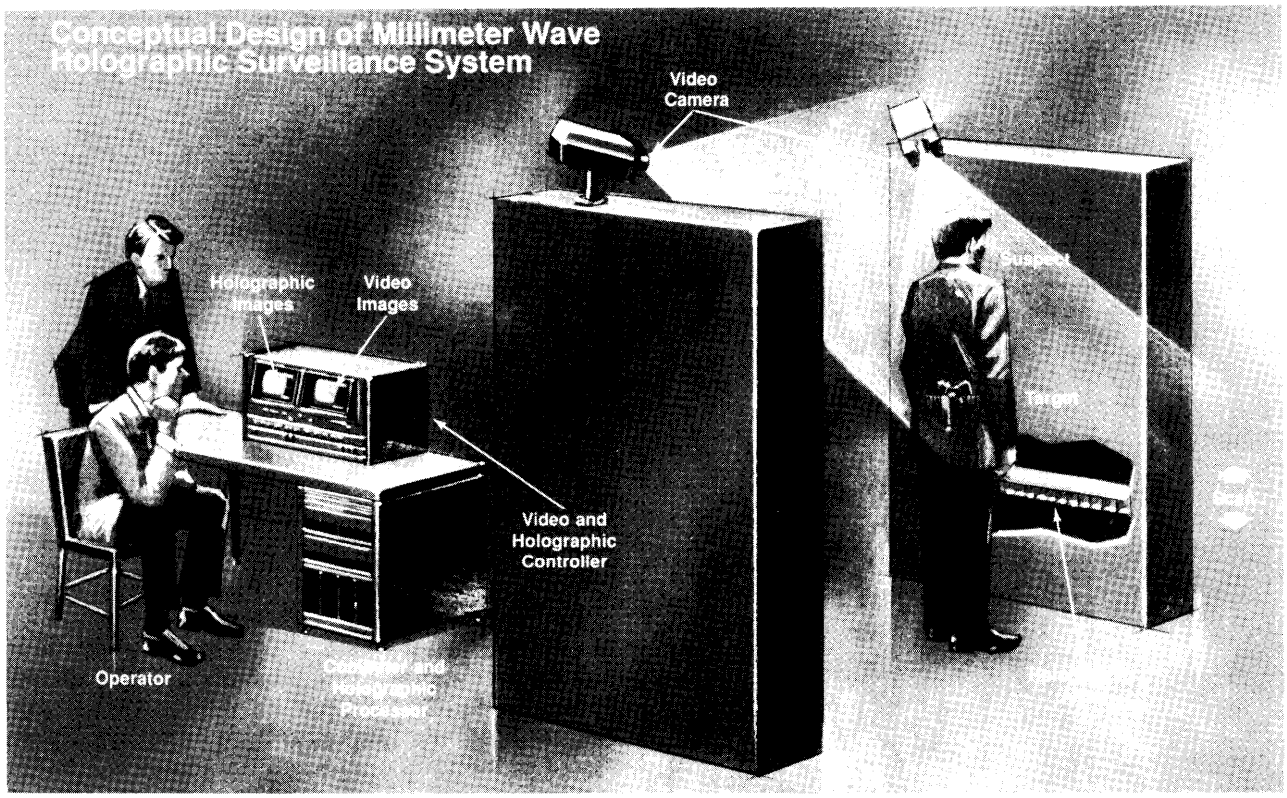
This section describes technology development by Battelle and Westinghouse. EVI, **a leading** designer of eddy-curent **metal** detectors, **is still** exploring conceptual designs for MMW weapon detectors. The General Dy**namics system was** developed for **a** different application. It is described in greater detail in chapter 7, **incident Response (SECRET); only aspects relevant to weapons detection are mentioned here.**

Battelle MMW

Battelle PNL is developing a "Millimeter-Wave High-Resolution Holographic Surveillance System" to permit security personnel to "frisk" suspects electronically and covertly for **concealed** metal **or** plastic weapons. Figure C-3 shows **an artist's** concept of **an** operational system. The device would obtain and **store in** computer memory **a** digitized millimeter-wave hologram **(a** three-dimen**sional image** obtained using coherent radiation) of **a "suspect"** (possibly **an ordinary airline** passenger) **re**corded by mechanically scanning the subject with **a linear array of** millimeter-wave antennas. Presumably the sus**pect** must be momentarily **still while being scanned-i. e., move no** more **than a** small fraction of **a** wavelength, which, **at** 35 GHz, **is** about 9 mm. Holographic images may be reconstructed **from the** stored hologram computationally and displayed **on a** computer graphics **terminal. An operator may select and change the depth at which the reconstructed image is focused. If desired, a closed-circuit TV image of the suspect maybe displayed on a separate video monitor.**

In 1989 Battelle demonstrated a developmental version of the system, obtaining the images shown in figures C-4 and C-5 by scanning the test objects in two directions with

Figure C-3—Artist's Concept of Millimeter-Wave Radar for Detecting Concealed Weapons



SOURCE: Battelle Pacific Northwest Laboratories, 1991.

a single antenna. Battelle is currently developing a linear array of antennas to permit recording of a hologram faster, in a single scan, and is investigating the possibility of a two-dimensional array real-time scanning system.

Westinghouse MMW Radar Technology

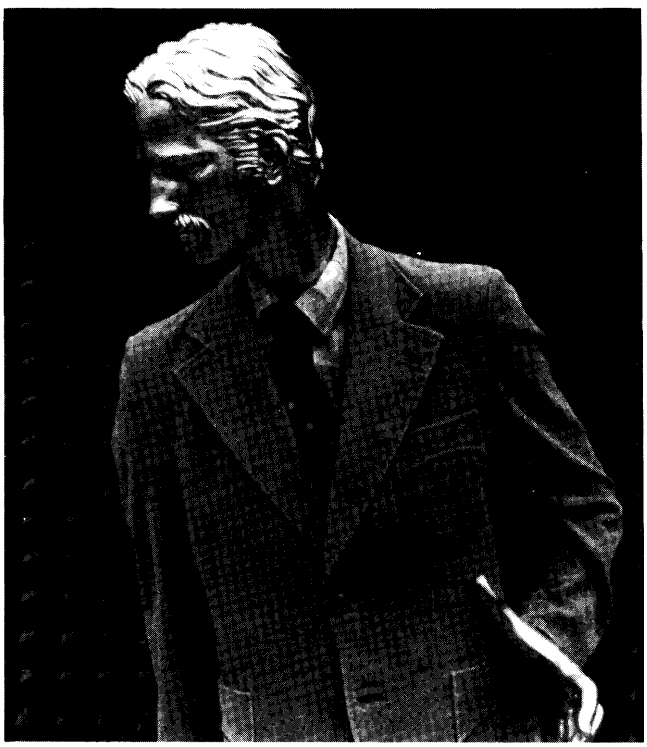
Westinghouse Advanced Technology Division in Baltimore is developing millimeter-wave radar technology applicable to weapons and explosives detection systems. The Westinghouse Electronic Systems Group responded to the FAA's Broad Agency Announcement of interest in weapons-detection systems by proposing to develop enabling components for a millimeter-wave weapon-detection system and to assess the potential of such a system. The system would use large (wafer-scale) gallium arsenide monolithic microwave integrated circuits (GaAs MMICs) similar to some that Westinghouse developed for DARPA and the Naval Research Laboratory (NRL). It would be used for short-range detection of weapons concealed on persons or in baggage.

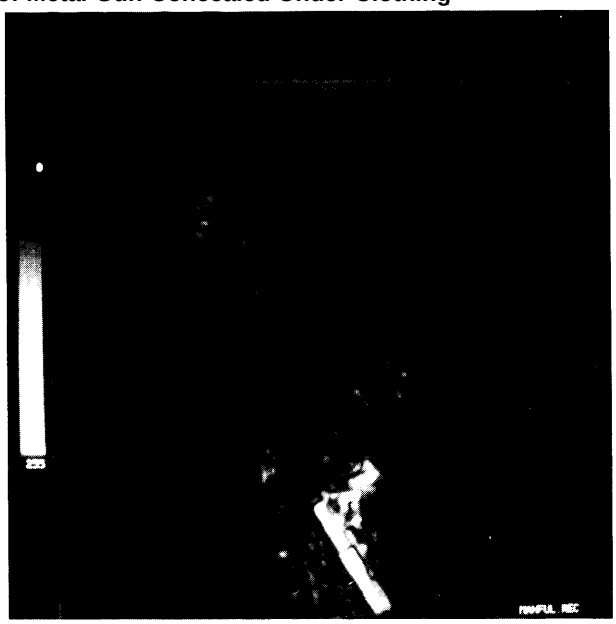
For the NRL, Westinghouse developed GaAs tiles (large chips), each containing an array of 16 antennas and integral detectors of 93- to 95-GHz millimeter waves. An array of such tiles was covered with a metal plate drilled with conical holes-one over each antenna-to concentrate received millimeter waves, increasing power at each antenna tenfold. The entire assembly would be used at the focus of a parabolic ("dish") reflector to provide a low-resolution image of millimeter-wave radiation sources.

For weapons detection, a similar system could provide imagery of millimeter-wave radiation reflected by weapon parts--e. g., a firing pin. Westinghouse estimates that a 10-milliwatt source would suffice for some applications and that the power-flux density of the millimeter-wave radiation at the target (e.g., skin) would be less than 10 milliwatts per square centimeter. Such an exposure, if shorter than 3 minutes, would comply with the current ANSI standard and NCRP guidelines. A weapons-detection system would include an appropriate millimeter-wave source.

Researchers at Westinghouse are interested in developing critical components-schottky-barrier diodes—for a weapons-detection system operating at 183 GHz. At this frequency, radiation from the source would be absorbed by the atmosphere in a much shorter distance than at 94 GHz, thereby reducing the potential of one weapons-detection system to interfere with a nearby one.

Figure C-4—Millimeter-Wave Radar Image of Metal Gun Concealed Under Clothing



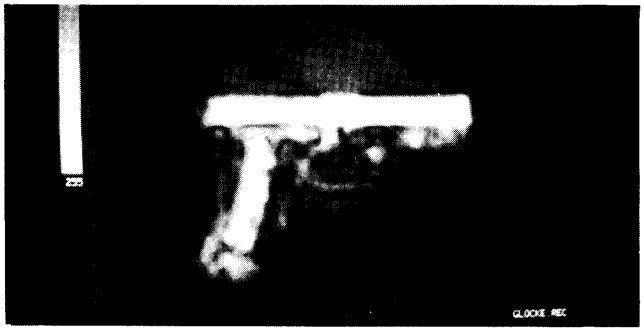


Left: Photograph of plastic mannequin wearing cotton/acetate suit concealing metal pistol.

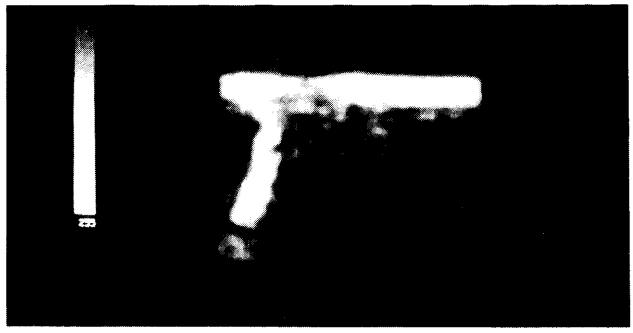
Right: 35-GHz radar image of mannequin and concealed pistol.

SOURCE: Battelle Pacific Northwest Laboratories, 1991.

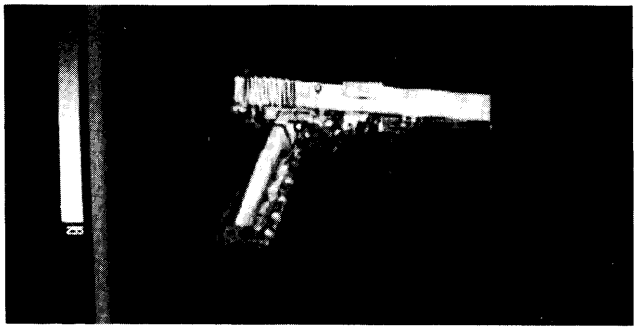
Figure C-5—Radar Imagery of Glock-17 Plastic-Handled Pistol



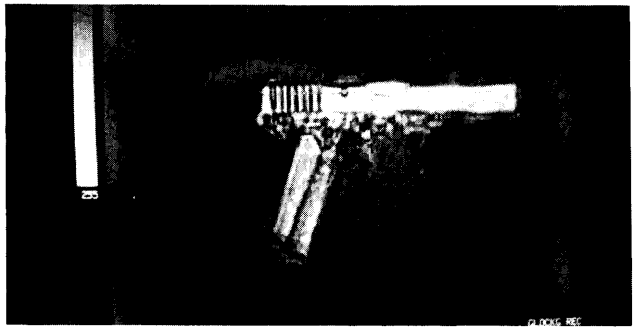
35-GHz radar image of Glock-17 pistol in air.



35-GHz radar imageofGlock-17 pistol behind one layer of heavy wool and one of light polyester fabric.



90-GHz radar image of Glock-17 pistol in air.



90-GHz radar imageofGlock-17 pistol behind one layer of heavy wool and one of light polyester fabric.

SOURCE: Battelle Pacific Northwest Laboratories, 1991.

Appendix D

Technologies To Protect Harbors, Ports, and Vessels

Introduction

A long list of obvious targets of potential interest to terrorists exists at the interface where land meets water. Shipping (especially cruise ships and ships with dangerous or expensive cargo), ferries, dikes, dams, levees, pipelines, oil platforms, cooling water intake ducts, canals, locks, ship yards, crowded beaches, coral reefs, oyster shoals, and other centers of ecological or economic value come immediately to mind. A more careful consideration, in addition, would highlight the importance of maritime industries to national priorities and their consequent attractiveness to terrorists. The importance of maritime trade is reflected in the fact that a very large proportion of the world's trade (by bulk) is carried by ships. In addition, millions of passengers board cruise ships every year.

Yet most Americans, if they contemplate the threat of terrorism at all, do not associate it with ports and harbors. Airplanes, embassies, and military facilities overshadow other targets in the minds of the American public.

Actually, attacks against shipping or other maritime targets are far from rare. Exact figures are hard to come by due to problems with data collection (many acts go unreported) and diverging definitions (e.g., terrorism v. piracy). But according to the International Maritime Organization, 179 known cases of piracy against merchant ships occurred between 1982 and 1989. Other sources claim that as many as 1,000 attacks have taken place from 1979 to 1989.[1] Some of these have been quite spectacular. In 1988,9 people were killed and another 46 were injured during a terrorist shooting spree aboard the Greek vessel City *of Poros. In* **May 1990, Libyan-based terrorists belonging to the Palestine Liberation Front of Abu'1 Abbas swarmed down in speed boats upon vacation beaches in Israel with the intention of directly attacking civilians along the Tel Aviv waterfront. Their mission was foiled by a rapid response by Israeli Naval, Air, and Land Forces, but only by the slimmest of margins.**

Despite their number, only a few of these attacks have won much notoriety within the United States, probably because few directly involved U.S. citizens either as victims or perpetrators. About the only exception is the 1985 attack on the Italian-flag cruise ship *Achille Lauro* (also organized by Abu'1 Abbas), in which **American Leon** Klinghoffer **was** killed.[2] The *Achille Lauro* affair touched off **a** lot of uproar including congressional hearings and court **actions that continue to this day.**[3] But the public **interest accorded this event is much more the** exception **than the rule.**

It is impossible **to determine with** precision why **there have not** been **more and costlier incidents involving our maritime industries. It is likely that something more than luck is involved. Insofar as the hijacking of transportation targets is concerned, several reasons for ruling out ships in favor (from the terrorists' perspective) of airplanes can be pretty easily formulated. For example, in the words of one analyst:**

> **. . .Terrorist and nonterrorist hijackings have plummeted in recent years . . . Takeovers of nonaerial means of transportation (buses, trains, and ships) have not risen to fill the operational void created by the decline in aerial attacks. [Byway of explanation:] Threatening to force the plane into a power dive credibly jeopardizes the lives of more individuals than does any comparable threat against other modes of transportation. Moreover, it is simpler to control the actions of a large number of people on board a plane in flight than it would be to prevent the escape of passengers from a ship.[4]**

Another points out:

> **Whether on the ground or in the air, an aircraft is more fragile than a ship by far, and the density of its cargo, passenger or freight, is high. It boasts of mobility on the order of forty times that of a ship, an important consideration in the hijacker's calculations of his chances for success. What is more, while high-value freight tends to be transported by air, more bulky, low-value commodities go by ship. The conclusion is easy to reach that ships are poor targets for hijacking compared to aircraft. Still, if a terrorist is seeking publicity as his primary objective, the uniqueness of a ship hijacking might have great appeal.[5]**

While some of the above arguments might explain why ships have been relatively immune to the threat of hijacking, it fails to explain why the American maritime

---

[1] M. Wisenhut, "Piracy and the Threat to USTRANSCOM," *Defense Transportation Journal*, vol. 46, No. 4, August 1990, pp. 16-18.

[2] For a good narrative account of this event see Scott C. Truver, "Maritime Terrorism, 1985,' *United States Naval Institute Proceedings, vol. 112, May 1986, pp. 160-173.*

[3] A court recently decided that the *daughters* of Mr. Klinghoffer were entitled to sue the PLO for damages resulting from the incident.

[4] Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (Westport, CT: *Greenwood press,* 1980), p. xxiv.

[5] R.W. Barnett, ' 'The U.S. Navy's Role in Countering Maritime Terrorism, " *Terrorism: An International Journal,* vol. 6, No. 3, 1983, pp. 469-480, at 472-473.

industry has been spared other forms of terrorism, for example: mass murder; or the destruction or the threat of destruction of other marine structures with concomitant economic and ecological damage; or ransom, for example of a multimillion-dollar vessel or an off-shore oil platform.

Few port authorities are so optimistic as to think that ''It hasn't happened here' can be reliably extrapolated to "It can't happen here." But even fewer sense any immediate need to reallocate perpetually limited funds from immediate, pressing issues to address what is currently a theoretical problem. However, as airlines toughen their security measures, as military and government facilities become better defended, as businesses abroad become more astute in providing security, as piracy and smuggling become a means to replace money formerly provided by East Bloc state sponsorship, as temptingly colossal new targets in the form of huge 5,000-passenger liners make their advent, and as the criticality of shipping to the support of our troops abroad (especially in the Middle East) becomes more apparent,[6] it is more than likely that terrorists will turn to untraditional, less hardened targets including ports, harbors and ships.

In addition to apathy, there are other impediments to the orderly implementation of further security measures around ports, harbors, and ships. One of these is confusion over responsibilities. As with any environment as complicated as a port, diverse authorities have hands in many facets of operations, including security. Should an incident occur, any one or several of a bewildering array of frequently overlapping and conflicting authorities could be involved, depending on the nature of the act and the location in which it takes place. Private security companies; port, municipal, local, State, and Federal law enforcement agencies; the U.S. Coast Guard; the U.S. Navy; the U.S. Customs Service; the Immigration and Naturalization Service; the Drug Enforcement Agency; port owners and operators; and the master and owner of each vessel all bear some measure of responsibility for security. Complicating matters, the rivers, lakes, and other bodies of water associated with ports and harbors frequently are used to define municipal, state, or even international boundaries. Therefore, it is not unusual to have to double or triple this already unwieldy list depending on the number of governments involved. And many other entities, including insurance companies, shipping companies, even passengers, unions, and the workers and crewmen they represent, clearly have a stake in a port's security arrangements.[7]

This problem is well recognized and some efforts are now being made to assign security duties unambiguously.

Legislatively, the Coast Guard bears primacy in the area of domestic port and harbor security. However, it is the FBI which is recognized as having primary responsibility for responding to terrorist incidents within the territory of the United States. In order to avoid confusion, these two agencies have signed a memorandum of understanding clearly designating the FBI as lead agency in the event of a domestic terrorist incident. A similar arrangement exists with the Department of State for response to terrorist incidents outside the United States. In the event of an incident, the Coast Guard would follow the direction of the lead agency and supply vessel, air and communication support, trained boarding personnel, and specialized expertise concerning maritime operations.[8] Another group, the National Port Readiness Steering Group, composed of representatives of the Maritime Administration (MARAD), the Coast Guard, the Military Sealift Command (MSC), the Navy Control of Shipping Organization (NCSORG), the Military Traffic Management Command (MTMC), the U.S. Army Corps of Engineers (USACE) and the commands of the Maritime Defense Zones (MDZ), is preparing a study, due out soon, with the goal of ensuring that in the event of a national emergency, the ports and harbors will be up to the task of mobilization. This study will result in a memorandum of understanding among the group members clearly assigning duties including security responsibilities. The group is also a conduit for the exchange of information and communication among its members.

But much confusion still exists among the many other players who face the myriad possible situations and disasters imaginable along the waterfront or on board a ship.

Many questions still remain. For example, while the Magnuson Act and subsequent legislation place ultimate responsibility with the U.S. Coast Guard, implementing regulations (33 CFR 6 et seq.) imply a somewhat shifted burden:

> Nothing contained in this part shall be construed as relieving the masters, owners, operators, and agents of vessels or other waterfront facilities from their primary responsibility for the protection of such vessels or waterfront facilities.[9]

Even in the absence of a coherent chain of command, some security measures are already in existence, although the main thrust of these measures is towards deterring and

[6] See H.W. Stephens, "Port Readiness for Military Mobilization" *Naval Forces,* vol. 9, No. 5, 1988, pp. 14-15.

[7] For more information see Hugh W. Stephens, "Barriers to Port Security, " *Journal of Security Administration, vol. 12, No. 2, 1989,* pp. 29-41.

[8] Admiral Joel D. Sipes, "Maritime Terrorism, " *Proceedings of the Joint Government-Industry Symposium on Transportation Security,* Williamsburg, VA, Mar. 21-22, 1990.

[9] 33 CFR 6.19-1.

responding to conventional criminal activities such as theft and smuggling. And there are several efforts under way to assess waterfront security needs and develop new equipment to meet them. As has been shown in our earlier report,[10] the first and best line of defense against any criminal or terrorist security threat lies not with technology nor with new machinery. Rather, there is clearly no substitute for vigilant, well-trained human beings alert to and reporting on suspicious activity. Still, to the extent that technology can assist these efforts, it should be supported. This appendix will describe technologies currently in use, on the drawing board, and just being envisioned for helping to ensure the safety of people and equipment in and around ports and ships.

U.S. Coast Guard Activities and Other U.S. Government Measures Against Terrorism

Any good security system, wherever located, must be capable of providing several functions, including prevention, detection, assessment, denial, delay, and response. In many instances, the equipment and procedures for providing these capabilities for land-based facilities are equally applicable to the marine environment. This is not particularly surprising since the two frequently face the same challenges: intrusion prevention and detection, contraband detection, access control, identity verification, site hardening, and so on. Many of these technologies are dealt with in appendix E and will not be further treated here except insofar as measures unique to the maritime environment are concerned.

However, one significant feature differentiates ports, harbors, ships, and other maritime structures from dry land: the presence of water. Water allows means of intrusion that find no parallel in considerations of shore security including swimmers, divers, fast surface boats, subsurface vessels (e.g., minisubs), and floating debris. This section will present some of the actions currently being taken and some of the technologies currently in place to combat the threat of terrorism in this environment.

Historically, the Coast Guard has borne the primary burden for domestic port and harbor security starting with enactment of the Espionage Act of 1917, although at the time this act was considered to apply only under wartime conditions.[11] In addition to its well-known inspection, with patrol, and safety functions, the Coast Guard administers several measures for improving port security by controlling access to port facilities, preparing contingency plans, and training personnel, which will be described below.

One of the most effective ways to prevent an incident is to block access to a vulnerable area. In addition to the obvious expedients of fences and locks, some means must be applied to permit entrance of authorized individuals while denying it to others. One of the current methods centers around the U.S. Coast Guard Port Security Card.

In 1950, President Truman signed Executive Order No. 10173 (later amended by Executive Orders Nos. 10277, 10352, and 11249) prescribing the creation of regulations "relating to the safeguarding against destruction, loss, or injury from sabotage or other subversive acts, accidents or other causes of similar nature, of vessels, harbors, ports, and waterfront facilities. ' This led to Part 6, Subchapter A, Chapter I, Title 33 of the Code of Federal Regulations: Protection and Security of Vessels, Harbors, and Waterfront Facilities.[12]

The only significant security measure engendered by these regulations was the requirement for persons seeking access to certain port facilities at certain times to possess an acceptable identification credential, most commonly a U.S. Coast Guard Port Security Card. This is a traditional picture ID with a signature and descriptive data. The card and surrounding procedures have been little changed over the 40 years of their existence and are now clearly antiquated. An applicant fills out a form and undergoes a background check. Problems with the card system include ease of forgery, relatively low durability, and, perhaps most importantly, lack of flexibility. Early court challenges established that wholesale denial of access to the general dock area by noncard holders was improper because such a procedure arbitrarily cuts off a worker from his livelihood. Therefore, the card system is now used (for official access control) only in areas of designated national security interest or under conditions of documented threat.

Controlling access to port facilities from the waterside is also a necessity although it is a little trickier. Insofar as overt waterside entrance is concerned, the Coast Guard has implemented various rules and regulations concerning entry into U.S. ports by foreign shipping, especially from what used to be known as the Eastern Bloc. However, terrorists, who have little interest in a long-term commercial relationship with their victims, would belittle inclined to advertise their arrival by voluntary compliance with these regulations. Still, to the extent that many terrorist groups operate out of known geographical areas and are likely to travel from these areas, these regulations do permit some control over the arrival of high-risk individuals. Routine controls by the U.S. Customs

[10] 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).

[11] This limitation was lifted in 1950 when the Magnuson Act (50 U.S.C. 191) amended the earlier legislation and madeport security a permanent Coast Guard duty. The Ports and Waterways Security Act (codified as 33 U.S.C. 1221-1227), passed in 1972, further broadened the Coast Guard's authority to take actions regarding security and provided some mechanisms for doing so.

[12] See also 33 CFR 125 et seq.

Service and the Immigration and Naturalization Service at all ports of entry help to deter and detect terrorist efforts to enter U.S. ports overtly from overseas. The Coast Guard is also involved in other counterterrorist efforts, primarily of an assessment and planning nature (see next section).

Role of the International Maritime Organization

In the aftermath of *the Achille Lauro* hijacking in 1985, the International Maritime Organization (IMO), which operates under the aegis of the United Nations, drafted proposed guidelines for security for passenger vessels and the facilities that service them (IMO Circular 443, published 1986). This proposal was largely the product of the United States' representatives (specifically, the U.S. Coast Guard and State Department) to the IMO. While the guidelines present a useful framework for assessing port security needs and implementing appropriate measures, they are strictly voluntary. The degree of compliance with the measures, both national and international, varies considerably from port to port but, while progress is slowly being made, concrete changes have generally been modest.[13]

The IMO measures were acknowledged and enlarged upon in the Omnibus Diplomatic Security and Antiterrorism Act of 1986, Title IX of which relates to International Maritime and Port Security .14 This law in part amended the Ports and Waterways Security Act, encouraged the President to continue to seek improved international seaport and shipboard security and suggested several measures to help reach that goal. The law also mandated that the Secretaries of Transportation and State produce various annual studies and reports on the topics of maritime terrorist threats and security at foreign ports. If the situation in a foreign port were found to be serious enough, and no remedial action were taken, issuance of a travel advisory was authorized. To date, no such advisory has been found necessary.

Congressional support for these measures has been minimal. For example, of the $12.5 million annual expenditure authorized by the bill, only $903,000 was appropriated in the first year.[15]

In large measure, implementation of the law fell to the Coast Guard. The text accompanying publication of the IMO Circular in the Federal Register[16] made clear that the Coast Guard intended to avoid across-the-board requirements, opting instead for a ship-by-ship and port-by-port appraisal and voluntary compliance. Other Coast Guard actions in support of the IMO Circular and the law included the creation and support of local Port Readiness Committees as a forum for coordination among the participating agencies concerned with the issues of port security especially where support of a military mobilization is concerned. The Department of Transportation is planning to issue regulations shortly for implementing IMO guidelines in the United States. In his 1989 report to Congress, the Secretary of Transportation noted that over 80 percent of the ports surveyed had established a Port Readiness Committee and over 50 percent of these included a Security Subcommittee.

The Coast Guard has also developed or supported several training programs designed to improve security awareness and capabilities for both domestic and international (under the Antiterrorism Assistance Program of the State Department) port authorities:

- Port Security Committees.
- Port Readiness Committees. The primary purpose of a Port Readiness Committee (PRC) is to "foster communication, cooperation and coordination among member agencies to strengthen the capability of commercial seaports to support deployment of military personnel and cargo in the event of mobilization or national defense contingencies."[17]
- Maritime Counterterrorism Contingency Plans.[18]
- USCG Training Programs.
- U.S. Training Programs for the Maritime Industry.
- U.S. Port Security Assessments.
- Foreign Port Security Assessments.

While these measures are laudable insofar as they go, they have been criticized as being too lenient and misdirected.

> . . . [T]o the degree Title IX and Coast Guard actions go beyond recommendations, the focus is upon inspections, training, and lighting, fences and other means to discourage casual entry. In their aggregate, these efforts suggest that government and industry have concluded that physical barriers and supporting practices designed to limit physical access to ports and ships are sufficient protection against plausible

[13] See "A Report to Congress on Passenger Vessel and Port Security, ' prepared by the U.S. Department of Transportation in compliance with Title IX of U.S. Public Law 99-399. This report evaluates national and international port and harbor security and is prepared yearly by the DOT as part of the United States' implementation of the IMO guidelines.

[14] 46 U.S.C. app. 1801 et seq. and 33 U.S.C. 1226.

[15] Stephens, op. cit., footnote 6, 1989.

[16] 52 *Federal Register*, 11,587-11,594 (1987).

[17] For more See A *Report to Congress on Passenger Vessel and Port Security* prepared by the U.S. DOT in compliance with Title IX of Public Law 99-399, Feb. 28, 1989.

[18] Ibid.

terrorist threats. Indeed, these may help to frustrate the isolated terrorist strike. But well-armed and trained terrorists or enemy special operations units bent on wreaking destruction and casualties will certainly not be deterred and scarcely inconvenienced by such measures.[19]

The Coast Guard is making some efforts to develop new responses to the threat of terrorism. Some of these will be described in the next section. However, in the absence of clear national priority or documented terrorist threats, it is unlikely that the Coast Guard will be allotted the resources to design and develop more exotic countermeasures.

In countering terrorism, forewarned is forearmed. Another service of the U.S. and other governments involves making sure mariners have up-to-the-minute information on factors affecting their safety. For some time now, it has been governmental practice to provide mariners with information affecting the safety of the shipping lanes including severe weather alerts, shipping lane blockages, and buoy or lighthouse changes. The Defense Mapping Agency is responsible for collecting and disseminating such Notice to Mariners. To do so, they have developed an Automated Notice to Mariners System (ANMS) containing information dealing with navigational safety. This system is part of DMA's Worldwide Radio Navigational Warning Broadcast System. Mariners around the world can connect to the system via satellite, telephone, radio, or computer hookup and access current information on a variety of topics. They can also file reports to be added to the database. In the early 1980's, the need for information about piracy and other attacks against shipping was recognized. Not only were these data of obvious interest to the mariners venturing into high-activity areas, but the governmental bodies charged with countering the threat of maritime terrorism had been hampered by the lack of accurate, comprehensive data on the magnitude of the problem. The U.S. Interagency Working Group on Piracy and Maritime Terrorism asked the DMA to expand its NAVINFONET system to include such warnings. With a few software changes, DMA complied with the creation of an automated message subsystem: the Anti-Shipping Activities Message File or ASAM of the Broadcast Warning System. Generally speaking, the incidents reported on this service are gathered from open sources such as newspaper accounts. Warnings and reports filed by mariners themselves are not checked for accuracy and NAVINFONET accepts no legal liability for the accuracy of the information. The purpose of the service is **to** provide warnings and this **mandate can be fulfilled even with slightly faulty data.**

There have also been initiatives from the private sector to beef up security. These are motivated not only by humanitarian concerns about risks to the lives and limbs of passengers and employees, and financial concerns about loss of property, but also by a rising consciousness of possible legal liability and insurance problems arising from failure to take reasonable precautions in today's hostile world.

> **Legal liabilities for negligent security practices are increasing and, as a result, the need for better maritime security is increasing. During the lo-year Persian Gulf War over 500 crewmembers aboard commercial vessels were either killed or wounded. These casualties have spawned all sorts of litigation, particularly in the United States, and one of the issues raised in these lawsuits is the seaworthiness of the vessels themselves. Insurance coverage very often depends upon the seaworthiness of the vessel insured at the time her voyage begins, and if it can be shown that a particular vessel was not seaworthy (that is, not fit for her intended use) because she was inadequately prepared for the security threats she faced, a precedent may be established which the maritime industry cannot afford to ignore. . . Shipowners, offshore installation operators, and port authorities are going to be held accountable in the future when their negligent security practices allow a terrorist incident to occur.**[20]

These security efforts have been primarily directed at **access control and baggage screening.**

About 3.2 million cruise-line passengers pass through the Port of Miami every year[21] **making it the largest cruise-line port in the United States. (Miami alone handles about one-third of all scheduled departures of major cruise ships from U.S. ports.**[22]**) At all the passenger terminals, the private cruise lines have provided x-ray and metal-detection equipment for screening all passengers and their carry-on luggage, much the way airlines do today. These units are not particularly expensive, as security equipment goes, about $120,000 per portal. But Miami alone needs about 12 of them to cope with its passenger flow. Furthermore, there are two gaping shortcomings in this scheme. First, there is no screening of checked baggage. Not only does this allow the emplacement of time bombs and other remotely operated devices but, unlike their airline counterparts, cruise**

[19]Stephens, *op.* cit., footnote 6, pp. 31-32.

[20]From ''Mva[e Security Services and the Maritime Industry,' a speech by Kenneth Gale Hawkes, Vice President, Maritime Security, Wackenhut Services, Inc., 1990.

[21]Captain Herman Gomez, Director, Training, Plarming & Development Seaport Authority, Port of Miami, personal communication, Oct. 11,1990.

[22]According t. the *Official Steamship Guide* as quoted in report on the hearing held Oct. 23, 1985 before the House Committee on Foreign Affairs on Overview of International Maritime Security.

passengers have access to their checked baggage, which is placed in their cabins before departure. Anyone who wanted to bring firearms aboard ship would not find it difficult. A second big problem is that passengers routinely disembark and reboard at ports throughout the cruise itinerary. Frequently these ports are either too small or too poor to offer much in the way of security services. Again, there would be little impediment to the smuggling of weapons or undesirable individuals on board by even the least resourceful of terrorists. Still, these measures by the Port of Miami are an important beginning.

One cruise line, Royal Viking, is taking matters into its own hands. It is arranging to equip its vessels with a portable security office: a small container furnished with x-ray and metal-detection equipment. The container is carried on board to be deployed when necessary. Returning passengers would pass through it as they reboarded.[23] Some cruise-line organizations are now considering bringing pressure to bear against ports in particularly risky areas by threatening to exclude such ports from their itinerary unless security is improved.

There are some problems with applying even these tried-and-true technological measures to port security. The environment around ports, harbors, and marine structures is particularly harsh: high humidity, salt water, motion, and storms are factors that find no parallel in the typical airport scenario. Therefore, it is not surprising that equipment for cargo and passenger inspection cannot be simply transferred from one mode to the other. Still, the concepts of x-ray and metal detection are viable although the implementation must be more rugged.

Insofar as self defense is concerned, civilian shipping generally employs few technological novelties. Many mariners are reluctant to bear weapons. They would rather not engage in literal combat with terrorists and pirates, seeing this as a task for the Coast Guard or Armed Forces who are better trained and better equipped for such activities. Generally speaking, this is the same approach recommended by the U.S. Department of Transportation's Maritime Administration whose position on the subject can be summed up in the title of its small brochure, *Piracy Countermeasures: Anticipate Trouble, Be Vigilant, Don't Be Heroic. The* measures suggested by this brochure are commonsense precautions such as posting guards, keeping unauthorized personnel off the ship, and making sure that the ship and surrounding areas are well lit. If pirates actually board, crewmen are advised to barricade themselves and any critical areas of the ship (e.g., the bridge) and radio for help. The most aggressive measure suggested by this brochure is the use of searchlights to dazzle suspected hostile boarding parties.

Some industry activists would like to see a little less passivity. A small but growing maritime security industry is specializing in assessing the vulnerabilities of port facilities and ships themselves and providing recommendations on measures to discourage criminal and terrorist activity. For example, Wackenhut, a corporation long involved with land-based security systems, recently started anew division devoted to maritime security. These recommendations include measures up to and including what sort of force to apply to repel unwanted boarders. High-pressure water hoses are a favorite.

Proposed Security Systems and Their Costs

U.S. Coast Guard Entry Cards

As previously noted, several deficiencies exist in the Coast Guard's antiquated identity card system. The Coast Guard is now in the process of developing and procuring a replacement for the current system to be known as the Port Access Control System (or PACS). This system will involve anew, more rugged and tamper-resistant identification card and a computerized local database. The card will not contain any visible identifying information but will be imprinted with a hidden computer readable bar code. At the time an individual applies for the card, a video image of the applicant will be made and stored on the database along with other biometric and identifying information. The cards will ordinarily be stored at the office of the local Captain of the Port. However, in times of emergency, they will be distributed to the port workers. In order to gain access to a controlled access area, a port worker would have to enter through a manned checkpoint equipped with a card reader. On inserting the card into the reader, a picture of the worker's face and other data appear on a television monitor where the guard can verify identity. By making use of computer technology, a system much more flexible than the current Port Security Card is possible. Access rights could be tailored to each individual's duties. Updating of information would be possible without having to reissue cards. Finally, tapes could be exchanged nationwide so that individuals found to be suspect in one area of the country could be quickly barred from ports in other areas. A prototype system has recently performed satisfactorily during testing and evaluation in New Orleans and is slated for further testing this year. Based on cost figures for the prototype, the Coast Guard estimates that each PACS will cost about $33,000. No finds are designated for this project in fiscal year 1991. A budget funding request for $2 million in fiscal year 1992 has been submitted for procurement and national distribution of the PACS to USCG field units.

USCG Underwater Sensing System

Another USCG innovation is the Surface Contact and Underwater Tracker or SCOUT, a multiple sensor system for detecting, locating, and identifying waterborne or submerged intruders. SCOUT is being developed jointly

[23] Norm Miller, ScanTech Corp., NJ, personal communication Oct. 10, 1990.

with the Naval Sea Systems Command. The novelty in this system lies **not with its instruments** and **sensors** that are **all conventional (sonar, radar, low-light closed-circuit TV), but the fact that they are integrated and carried on a mobile platform, specifically a van. This allows coverage of a large geographical area with only a few units. SCOUT is expected to be deployable by the end of fiscal year 1992. An enhanced workstation for optimizing sensor placement is expected in fiscal year 1993. The frost unit will cost about $2.5 million. Additional units, assuming no major overhauls, would run about $1 to $1.5 million each.**

Underwater Acoustical System

Finding **an** underwater intruder **is a** difficult **task** Human hearing **was** designed **to** operate in air and is less effective when immersed in **water. Sight is limited by water turbidity, particularly in many ports. Regular human patrols of the immediate area are usually not feasible. Therefore, detection of unauthorized swimmers or submersible craft must depend on mechanical surveillance. Several systems for this purpose have been proposed.**

A major problem with controlling access from and through the water is that few means for reasonable escalation of force are currently available, Once detection is accomplished there are few options short of deadly force to deter or stop an intruder.

One corporation, GT-Devices, a subsidiary of General Dynamics, is trying to interest the Navy and other authorities in their system, which, they believe, can stop an intruder without use of deadly force.[24] The Underwater Deterrent Security System is advertised as a nonlethal human-swimmer defense system. It is based on an array of electrothermal sources that would be permanently emplaced underwater. The sources are capable of quickly generating energetic plasmas and thereby producing a high-intensity, directional acoustic emission. The magnitude and direction of the pulses are supposed to be adjustable. The acoustic pulses are generated by the rapid (microsecond time scale) discharge of high energy (on the order of kilojoules) electrical pulses. These cause explosive formation of plasmas in the water and resultant pressure waves. Several plasma generators are organized into a phased array. The company has actually produced a 16-generator array for testing purposes. By controlling the amount of power to each plasma generator, the magnitude and direction of the resulting pressure pulse and the location in which the pressure waves combine to reach maximum intensity may be controlled. At low power, the pressure waves may be used as sonar to detect, track and range. As power and pulse repetition frequency are increased, the effects of the system **increase, going from** unpleasantness **to** pain **to** physical injury. Because **it can be** focused, the manufacturer **asserts that** collateral damage **to** adjoining **structures or** organisms **can be** controlled. The useful range **of operation for the steerable device is up to 1.5 kilometers from the fixed underwater installation, according to GT-Devices. Some** observers are skeptical **of this estimate. The true effective range would have to be determined by testing in open water.**

The system has demonstrated (in the laboratory) an ability to bend metal, indicating that it may also be suitable for deterring intrusion by underwater craft. The system is reported to operate with a 4-kilowatt generator, although the generator size will depend on the desired range. The Navy, for example, is interested in a 600-meter warning zone and a 200-meter keep-out radius. With their test array of 16 emitters, the manufacturer indicates that the system can achieve a focus spot only a couple of meters wide at a range of 200 meters.

Following an initial development contract, the Navy has not been interested in supporting this technology further, making several arguments. First, that it still needs too much money to get to advanced development. This would be inconsistent with the Navy's ''off-the-shelf" philosophy. The Defense Nuclear Agency has shown some interest in the project, but would have to cancel other programs to pay for it. It is said to use too much power in a realistic configuration. Further, its function comes under active denial, which is handled by the Air Force. The focus is at a preselected distance and spot and the beam is very narrow. The Navy asserts that it would need a unit every 100 feet or so.

The Navy Waterside Security System

Following several intrusions in 1984 at the Electric Boat facilities in Groton, CT, where much of the Navy's nuclear powered submarine development work is carried out, the Navy decided that current waterside security capabilities were inadequate. They felt the need to improve their ability to detect, assess, and respond to intrusions by high- and low-speed boats, surface swimmers, scuba divers, and explosives and other inanimate threats hidden in floating debris. In conjunction with the Coast Guard, NASA, the Department of Energy and the Canadian Government, the Navy set about developing an integrated, multi-sensor, automated system, dubbing the project the Waterside Security System. The plan originally envisioned a nearly fully automated and integrated system whereby, for a site the size of the submarine base at Bangor, ME, a single human operator could monitor the waterside security status for the entire installation. The operational requirements of the system were:

[24] See N.K. Winsor and R.B. Ashby, "Underwater Deterrent Security System (UDETSS),'' GTD-90-2, 1990.

Underwater and surface swimmer	Detection to 200 yards @ 0.90 detection probability
Surface craft	Detection to 1,000 yards @ 0.95 detection probability
Operational availability	0.90
False alarm rate (FAR)	1 per 2 hours
FAA (long-term goal)	1 per 8 hours
System cofilguration	Fixed and transportable

The first approach attempted to use off-the-shelf technology as much as possible. This generally turned out to be possible for the sensing systems that consist of sensitive but conventional radar, closed circuit television (both normal and low-light systems), and forward-looking infrared (FLIR) detectors. An exception to this rule was the sonar system, which requires some developmental work. The communications, command, and control (C^3) system has turned out to be more complicated. No off-the-shelf system was capable of providing the automatic targeting and alarm capabilities the Navy felt were critical to successful implementation. With the help of the Canadian government, which has funded about 55 percent of the research and development costs of the C^3 system, the Navy expects to test systems operation in 1991, perform additional testing in 1992, and field operational systems in 1993.

It does little good to know that an intruder is present if there is no way to deter his mission. One problem in the waterside environment is the lack of credible, escalatable countermeasures. Frequently, commanders find that there is little in their arsenal short of deadly force (e.g., dropping hand grenades in the water) with which to respond to a waterborne threat.

The Navy is working to develop several such measures. The first is straightforward: light. Not only is it harder for a intruder to get away with his plan when the targets of his malfeasance are well illuminated, but, the Navy has found, with sufficient power, light itself is capable of delaying, even disorienting, an intruder. For this reason, part of the Waterside Security System consists of a 4-million-candle-power lighting system capable of casting a beam over a mile. Like the other parts of the system, the high-power lights are controllable from the console of the security watchman.

Another response measure on which the Navy relies is marine mammals. The animals can be trained to do many of the actions for which police departments frequently use dogs. They can detect intruders and raise an alarm. They can also be trained to act aggressively towards an intruder. Training and maintaining marine mammals is not easy, however. Unlike dogs, marine mammals are not pack animals and are not motivated by a desire to please the putative pack leader (the trainer). They will work for food but when their hunger is satisfied or when they get tired, they stop. It takes about 2 years to train a dolphin and, of course, there are considerable costs connected with the care of the animal once it is released to service. Still, to date, many Navy security personnel consider patrol by marine mammals one of the most effective measures available.

A comprehensive security system includes delay tactics as well as detection and response components. Toward this end, the Navy is working on development of waterside barriers. A 1985 effort aimed at a barrier capable of stopping a high-speed boat would have cost $2,000 per foot (just for hardware and installation; maintenance was extra). Antiswimmer nets are similarly expensive and invoke a host of environmental problems. The United Kingdom, facing a very real threat from IRA terrorists, has been willing to make large investments in barriers. The Navy would like to be a little more frugal. Still, for a fast boat attack, the Navy recognizes that a barrier is the only defense option. There is no time between detection and disaster to formulate any other response.

Work is now going on to develop a rapidly deployable (on the order of a day), low-cost (on the order of $200 per linear foot) barrier capable of stopping a 50-foot cigarette-type boat approaching at 45 knots. The latest model is down to a promising $500 per linear foot with most of the cost arising from the preparation of permanent mooring fixtures on the bottom. This kinetic barrier, a floating arrangement of PVC piping and wire, has a submerged foil. When struck at high speed, the foil "digs" into the water, causing the barrier, and with it the speed boat, to flip over. Scale models have been tested at California Polytechnic University, San Luis Obispo, and full-scale crash tests are planned shortly at Port Hueneme, CA. This approach has several advantages. Except for the moorings, the system components can be stored in a protected environment. This sheltering from the elements substantially reduces maintenance costs. In the event of a documented threat, the barrier can be installed fairly quickly and on a' 'low-tech' basis. The moorings, on the other hand, even in the absence of the fencing, are useful for clearly defining the security perimeter. Such a clear demarcation is a useful legal tool for specifying what level of action is appropriate at what distance from the facility.

Appendix E
Physical Protection Systems

Introduction and Summary

Typical fixed-site targets of terrorists are private corporations' assets (e.g., buildings, pipelines, electric pylons), vehicles (planes are a current favorite), bridges, monuments, and diplomatic buildings.

Since a terrorist can seldom be identified before the act, the first line of defense against terrorists is usually proactive physical protection of the target (a barrier between the terrorist and the target). Depending on the degree of protection needed, the physical protection may range from a simple wall or fence, such as a boundary marker, to a sophisticated physical protection system (PPS). A physical protection system is a collection of system elements, combined to achieve protection according to a plan. The classical physical protection system incorporates two substantial surrounding fences with a clear zone between and includes many high-tech sensors and interconnecting communications.

Physical protection systems at different sites are seldom identical because of the differences in facilities, targets, and threats. The basic design for physical protection systems is quite well established but considerable engineering and design tailoring is usually required for each site.

The four basic functions of a modern physical protection system are:

- **entry control,**
- **. detection of the intrusion,**
- **. delay of the intruder, and**
- **• response to the intrusive action.**

All of these elements must be present in any effective physical protection system to the degree necessary to meet the threat expected. The last three functions must be performed in sequence and within a period of time that is less than that required for the adversary (i.e., terrorist) to overcome the physical protection system and commit the act (e.g., property destruction, kidnaping and hostage taking, personal injury, or murder).

The components of a physical protection system will be discussed in more detail below. Elements to be presented include description, applications, technology, operational limitations, existing deficiencies, development status and activity, costs, and expected new capabilities.

Threat assessment is usually the first step in any physical protection system design, followed by site assessment, physical design, construction, operation, and functional assessment. The system elements must be balanced so as not to create weak links. For example, an adversary is not likely to take time to burn a crawl hole in a steel door if the hinges can be easily dismantled. Several useful computer programs are available to aid in assessment of specific site security plans and in the design of a protection system (e.g., SAVI, ASSESS, and SENLAX are a few available at Sandia National Laboratories).

A physical protection system can also provide deterrence because it may be viewed by the terrorist as a formidable object requiring many tools and people to penetrate and thus may result in a delay in his plans, or better, a decision on his part not to act at all. Deterrence, however, is difficult to measure and cannot be depended on.

Brief Assessment of Current Physical Protection Technologies

Except for explosives detection, the technologies and hardware for entry control into a protected area are available and are reasonably adequate for screening personnel and packages.

The common and widely used coded photo badge technology is mature but, by itself, provides minimum security.

A variety of high-security identity verifiers based on personal biometric features are now available and functionally adequate for personnel screening. They are more reliable than using guards to screen entrants, especially for large populations and are operationally less expensive, but they do not present the deterrent and response value of guards.

The technology for metal detectors is mature; they are available and substantially adequate for most weapon screening except for a few selected handguns.

The familiar x-ray package search machine is widely used but some kinds of explosive devices are difficult to detect. Nuclear radiation-based detection systems are still bulky, expensive, and slow. The sensitivity can be set to detect a small mass of explosives if the corresponding false alarm rate can be tolerated.[1]

A perimeter system of a large physical protection system typically consists of two 8-foot chain link fences spaced about 30 feet apart with the area between graded

[1] See the first report in this series, 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), p. 10.

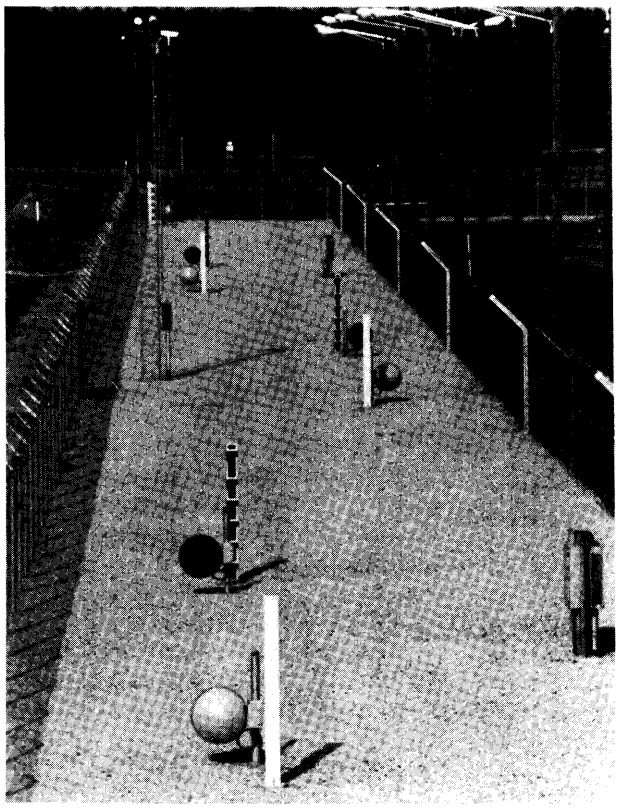


Photo credit: Sandia National Laboratories, 1990.

View of intrusion detection and assessment system.

and covered with rock. A disturbance detector (perhaps a seismic or a taut-wire sensor) is attached to the outer fence and one or two overlapping intrusion detectors, such as an electric field sensor and a beam type sensor are located between the fences. An array of surveillance TVs with matched lighting is typically also installed in this ''clear zone," (see figure E-l). All sensors are then connected to a common alarm, assessment, and control center. The cost of such a perimeter system is typically about $1,000 per foot.

Tests have shown that some barriers that appear to be impenetrable can be breached quite rapidly by determined terrorists who are trained and well equipped.

Although some improvements are being made in the more conventional structural barriers in terms of materials, designs, and construction, more visible technical advances have been achieved in the unusual quick-deployment barriers. These more exotic dispensable-on-command barriers are less developed, but first-generation versions are available for tactical and special defensive applications.

A risk in the use of quick deployment barriers, however, is that in addition to containing or slowing down the terrorists, they may also create a difficult escape path for the evacuees and the response force.

Reliable intrusion sensors are readily available from several suppliers. They are used extensively as single units and in multiple-unit networks in detection systems of all sizes. Internal-intrusion detectors, usually involving the use of a different set of sensors from those deployed along external perimeters, are usually mounted on the walls, windows, or doors of a building. Intrusion detectors are often used in overlapping arrays for mutual protection and reliability.

Closed circuit television (CCTV) is usually used for the initial assessment of an alarm. TV in a large system is usually cost-efficient since one person can monitor several areas at the same time from one central location.

Based on the principle of detection, delay, and response, Sandia Laboratories has developed, under the sponsorship of the U.S. Army RD&E center at Fort Belvoir, a medium-size, flexible physical protection system named SAFER that is quickly deployable on command. It was developed primarily to protect field sites and high-value military assets deployed in antiguerilla or countemarcotics operations. The system hardware is procured and stored in kit form and costs about $360,000 per kit. Each kit consists of infrared sensors, both passive and active, seismic sensors, an assessment platform with low-light TV, and a public-address-system speaker. A video display console is included. The system also includes a razor-tape concertina type of wire barrier, hand-held radios, electromagnetic fence-disturbance sensors, and night-vision binoculars. The kit may be retrieved for redeployment. Several have been procured and stocked and more are scheduled for procurement in 1991.

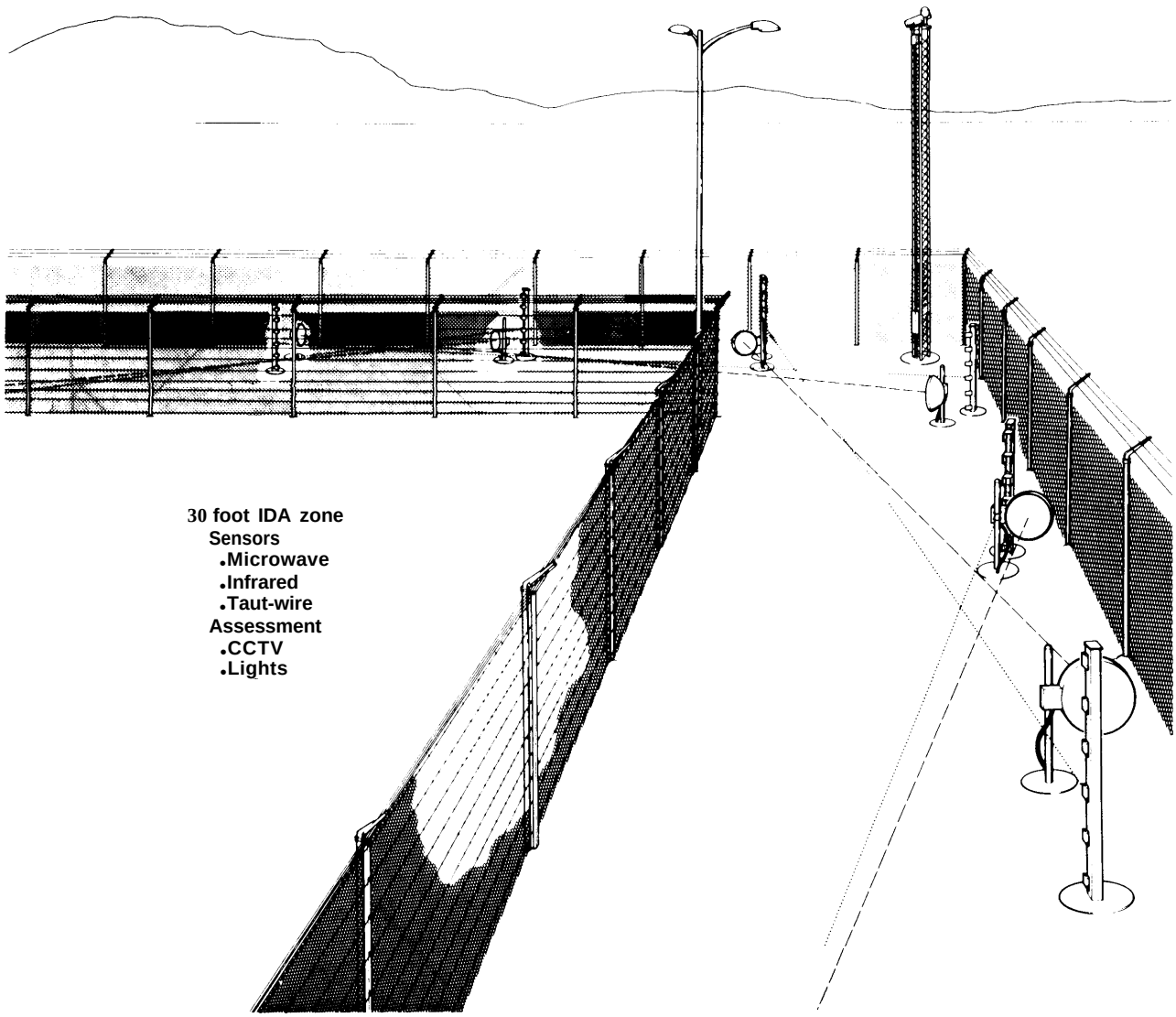
Entry Control

Entry control refers to the admission of authorized personnel to and the blocking of unauthorized personnel from a physically protected area; it includes screening personnel and material.

After a perimeter barrier is established around any protected area it must be provided with an entrance and exit corridor for the movement of personnel, material, and equipment for operation and maintenance. This entry control corridor must include a screening and separation enforcement system. Such systems range from totally manual to fully automatic and may be used for screening on the way out of as well as on the way into the area.

To prevent theft, sabotage, hostage taking, or other terrorist acts, it is necessary to search for concealed contraband, not only on persons but also in packages and vehicles passing through entry control. The items usually looked for are weapons, explosives, drugs, strategic and precious materials, special tools and parts, and hazardous

Figure E-l—Intrusion Detection and Assessment System



SOURCE: Sandia National Laboratories, 1990.

materials. Hand-searching, with or without hand-held sensors, is usually too slow or socially objectionable for a population of more than a few.

Personnel Screening, Manual

In a fully manual screening system inspection is done by a guard or security inspector on an individual basis.[2] At a facility where there are many authorized persons and the guard force is large, this system becomes ineffective and impractical without at least some minimal aid, such as the familiar photo badge, which is frequently coded for machine reading. The use of the photo badge requires that the screening guard make only a comparison between the person's face and the photo for admittance. This system assumes that the badge is authentic and is being presented by the authorized user. In the interest of cost and at additional risk, this comparison is sometimes accomplished remotely using closed circuit TV. Heavy dependence on the photo badge can be a security risk for several reasons: 1) photo badges can be counterfeited, 2) an impostor's face can be made up to match the photo on a stolen, borrowed, or found badge, 3) the guard's inatten-

[2]An example of such a system is at OTA, 600 Pennsylvania Avenue SE, Washington, DC.

tiveness due to boredom, distraction, preoccupation, etc., can make his activities ineffectual. However, as a first line of personnel screening the guard-plus-photo-badge system is often adequate and such systems are well developed and widely used. Photo badges cost from about $1 to $10 depending on the amount and kind of encoding used.

The cost of a full-time (three-shift) guard position is about $185,000 per year. Therefore, in the interest of cost saving, to say nothing of security quality, a reduction in the size of the guard force at entry control locations by using a machine-aided or fully automatic screening system may be attractive. A machine-aided system, for example, using a coded photo badge and a badge reader and leaving only the final approval for each entry attempt to the guard, may speed entry, improve security, and, in the long run, reduce screening costs. A much greater economic advantage may be gained from the use of an automatic screening system.

Personnel Screening, Automated

An automated entry control system, usually with only guard overview, can make use of personnel identity verification devices for screening. Such devices make a close assessment of a personal biometric feature, such as a hand profile, a fingerprint, a voice pattern, a retinal pattern, or the way a signature is written, then automatically compares that verification sample with a previously stored reference sample of the same biometric feature. These devices have existed in development form for a decade and are now available from several manufacturers who can supply not only hardware and software but also the necessary spare parts and technical assistance for installation, operation, and maintenance. Indeed the supply of a variety of functionally adequate identity verifiers is now available to fill the requirements of the security industry. The capital cost of a typical personnel identity verifier ranges from about $1,000 to $5,000 per verifier, which is generally small compared to the total cost of an operational entry control system. The total cost of using verifiers must also include not only machine procurement, but also installation, maintenance, user instruction, user enrollment, and many times the design, procurement, and installation of a management-system network.

The number of verifiers required in an entry control system depends on the speed of the verifier, the number of personnel to be screened, the number of portals, and the patience of the waiting users. Verified performance tests show that about 3 to 7 seconds are required for the verification of a claimed identity. A false acceptance of an unauthorized person and a false reject of an authorized person can occasionally occur, but broadly speaking, the frequency is less than 1 percent. These error rates are interrelated, however, and are dependent on machine adjustment. This kind of accuracy is acceptable for most well-designed entry control systems. More accuracy and speed and less cost is desired, of course, and those goals are the object of current development efforts.

The use of an identity verifier, now commercially available, in place of a guard is usually cost-effective but can also be justified because of fewer errors and better reliability. The deterrence associated with guard presence may be lost if the guard position is totally eliminated in favor of a verifier. However, some security personnel are generally required to oversee the screening operation, help visitors, provide occasional help for the handicapped, care for equipment breakdowns, prevent vandalism, and be available to challenge a suspected impostor.

Successful operation of the verifiers requires cooperation on the part of the user and a minimal amount of operator skill. A personnel screening machine, such as a facial-recognition device that could be used nonintrusively to scan a succession of people at a port of entry or at an airport security screening portal, would be extremely useful to search for certain wanted persons. For example, a known terrorist, who had previously been registered into the recognition system from a photograph could be covertly identified with such a system. With the recent advent of neural networks and other powerful algorithms,

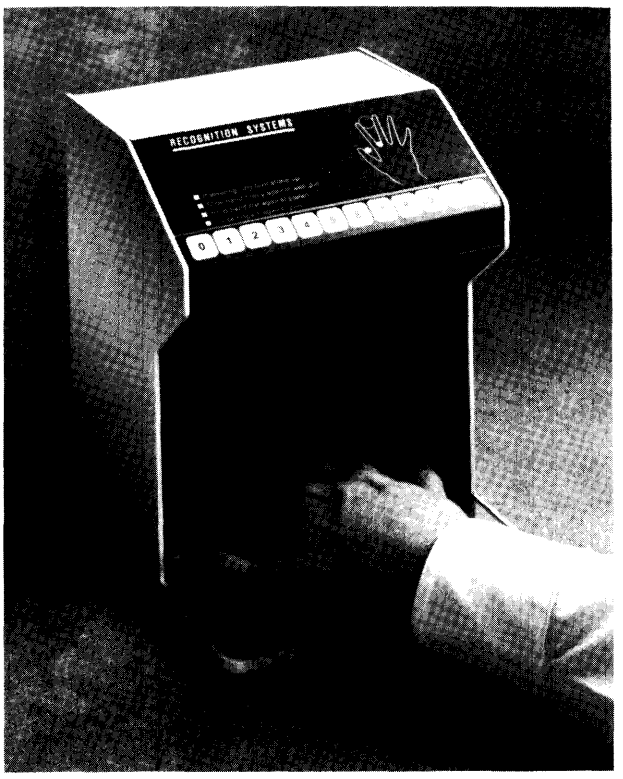


Photo credit: Sandia National Laboratories, 1990.

Hand profile identity verifier.

Photo credit: Sandia National Laboratories, 1990.

Fingerprint identity verifier.

several facial-recognition systems have been developed to a prototype state. Two developers are David Sarnoff Research Center in Princeton, NJ, and International Imaging Systems in Milpitas, CA. No device is yet commercially available.

Entrance barriers in an entry control corridor, including intrusion-resistant doors and turnstiles with associated latching hardware that can be operated remotely, have been in use for years. However, the technology required to insure that only one person, the person whose authority has just been verified, passes through a single door when it is released, is not yet commercially available. The two-door-portal assembly is an operationally adequate device for this entry control task, but it is bulky (3 to 5 feet square), slow (about 20 seconds per entry sequence), expensive ($20,000 to $60,000 per portal), and not widely available. The development of a much simpler, faster, and less expensive doorway monitor is needed.

Weapons Detection

Terrorist activities frequently involve the use of weapons and tools, usually made of metal. Therefore, an entry control system must also screen for unauthorized metal objects that may be carried on a person. The hand-held scanning metal detectors are the most sensitive but their use is slow and manpower intensive and

therefore not practical for screening large populations at a reasonable rate.

The basic portal metal detector has changed little in a decade. It senses a change in an electromagnetic field pattern when a metal object is moved into the active area of the portal. The pattern is sensed after a short electromagnetic field pulse is applied by the portal electronics.[3] The sensitivity of a weapon detector is effected by the weapon's shape, size and orientation, the kind of metal used, the size of the carrier, velocity and direction through the portal, and by other objects in and near the sensing magnetic field. Recent improvements, primarily centered around sensing only during various "time windows" after the interrogating pulse, have provided more sensitivity and more stable operation than previous models were able to attain. The metal detector is limited by its inability to distinguish between a weapon and a piece of innocent metal of the same or smaller size. It may be reasonable to expect that continued development will produce a metal detector that will find these weapons among other pocket clutter but it is unlikely that it will ever be able to find the emerging totally nonmetal gun, in the absence of metallic tags emplaced by the weapon manufacturer.

A software program is being developed for metal detector operation that will provide high sensitivity, regardless of the kind of metal (e.g., iron, copper, zinc, stainless steel, or aluminum) being passed through the portal. There is also some continuing effort toward the development of a very low-power microwave imaging device that will be able to search for high-density objects under clothing (see app. C).

The (regulatory) magnetic field intensity limitation of 1 gauss for metal detectors is restrictive and imposes limits on sensitivity and accuracy. However, in spite of its limitations the use of metal detectors at airports has apparently been effective in greatly reducing the number of weapons carried onto aircraft, as evidenced by the reduction of skyjackings in recent years. The cost of a portal-type weapon detector is about $6,000.

Explosives Detection

Explosives detection has been discussed in detail in the first OTA report of this study and in chapter 4 of this report and so will be discussed only briefly here.[4] An explosives detector is necessary in an entry control system because explosives are not only commonly used by terrorists for forceful entry but also for sabotage and injury within a protected area. Explosives detection is complicated by the variety of carriers to be searched such as personnel and their clothing, briefcases, packages, tool boxes, instruments, and other places where explosives can be hidden for smuggling. The basic methods used for bomb detection are explosives-material analysis (vapor and solid) and object identification with the aid of x rays and hand searching. Important features of a good searching system are high sensitivity, high resolution, high scanning rates, low false alarms, and safety.

Explosives Carried by Personnel

The material-analysis techniques being developed for explosives detection are based on well-known physical and chemical properties of explosives. Currently available explosive-vapor detectors, which use the only automated technique now acceptable for searching people, cannot detect all types of explosives that might be used by a terrorist. Several hand-held detectors based on explosive-vapor collection, concentration, and analysis are commercially available. The use of these devices, however, is manpower intensive and slow. Further, the devices are not sensitive to all types of explosives. However, technical developments in this area have become rapid and new, radically improved devices are now available.[5]

Package Search

For packages, a conveyor-belt search system, as seen in airports for baggage inspection, is frequently used. This scanning system, using x-rays, is limited to generating video images of concealed objects (of various densities) which, if suspicious, must be further assessed by inspectors. This technique relies heavily on the operator. Much attention is now being given to alertness enhancement techniques (part of human factors applications-see ch. 5) such as frequent rotation of inspection personnel and a reward program for the detection of planted test objects. Various x-ray inspection aids, such as color and image enhancement, zoom control, and density highlights are available.

Modern x-ray inspection systems, such as those found at airports, are designed to insure radiation safety. First, the x-ray dose per package scan is very low compared to medical and dental sources. Radiation shields effectively limit radiation levels anywhere immediately external to the search machine to less than 0.0005 Roentgens per hour, which is much less than the maximum allowable set by the Bureau of Radiological Health and Safety. By comparison, cosmic radiation at 35,000 feet is 0.0001 Roentgens per hour or more, so a passenger will receive far more radiation from a high-altitude flight than from x-ray screening of his luggage prior to boarding. These

[3] See app. C for more detailed discussion on metal and weapons detectors.

[4] U.S. Congress, Office of Technology Assessment, op. cit., footnote 1, chs. 4-5.

[5] Ibid., chs. 4-5 and app. C.

radiation levels are not damaging to pharmaceuticals, computers, magnetic tape, food, or and almost all other substances.[6]

Dual-energy x-ray inspection, as the name implies, makes use of two x-ray beams of different energies. This system, besides obtaining item profiles, can also provide information about an object, such as atomic number, when the images of the two beams are compared. By exposing objects to two or more x-ray beams from different directions, three dimensional information can also be obtained (this technique is called tomography). By employing computer processing the maximum image information can be obtained for better item identification. Dual-energy computerized tomography is well developed for the medical industry but is expensive. The radiation backscatter variation of x-ray imaging from materials of different density is also useful in identifying scanned materials. Minimal success has thus far been gained in the development of a computerized system using using neural networks for object recognition from the x-ray image. A fully automated x-ray system, without the human discriminating link, is not yet available, although one firm, AS&E of Cambridge, MA, claims to be close to marketing such a system.

Neutrons of normal thermal energy can also be used to screen packages for explosives materials. The procedure involves exposing the package and its contents to a very low dose of neutrons which interact with nitrogen to generate characteristic secondary radiation, which is detected. Such a machine was developed by Science Application International Corp. and sponsored by the FAA Several of these very large baggage search machines were then built at a cost of something over a million dollars each.[7] The use of high-energy neutrons in a similar system is being considered by other developers. The use of other types of radiation for package searching is an interesting and promising technology but further development is yet required to provide a practical time-efficient machine for the detection of explosives at airports.

Searching for explosives in vehicles such as cars and trucks is usually done by hand searching and sometimes with the aid of hand-held vapor detectors or with wipe patches that are later analyzed for traces of explosives.

Dogs are still used to determine the presence of contraband. Their sniffing time span is quite limited (about 20 minutes per session) and they are strongly dependent on interaction with a specific handler, thus making their availability and use relatively costly (see app. B).

Development activities in the area of explosive detectors has, in the last few years, improved sensitivity and reduced operating times by factors of 10 and 100. However, so far the urgently needed fast, sensitive, and accurate explosives detector for personnel and packages searches has not arrived. A practical and reliable detector for the more commonly used bomb explosives is urgently needed.

Reference 1 in the bibliography to this appendix contains additional information about entry control technology.

Intrusion Detection

Detection is the discovery of an intrusive action at any point in the protection system. Detection is usually reported by an intrusion sensor and announced through the alarm communication subsystem. The intrusion alarm must then be followed by an assessment; if appropriate, the response force will then be notified.

The detection of an intrusion or an attempted intrusion into a protected area is one of the four basic functions of a physical protection system. It is important to make this detection as soon as possible after the start of the intrusive action to provide the maximum time for assessment and response. Maximum delay usually means detection as far from the target as possible.

Exterior Sensors

Several fence-disturbance sensors have been developed to detect attempts at fence scaling or cutting. Personnel and vehicles used for forceful entry by ramming the fence can usually be detected by the same exterior sensors.

A fence disturbance caused by climbing can be detected by special sensors fastened to the fence. The heart of one such sensor consists of a magnet-and-coil arrangement; another utilizes piezoelectric crystals. These measure slight disturbances in the geometry of the fence caused by the intruder. Another relatively unsophisticated sensor utilizes a taut wire, usually barbed wire, stretched along the inside of the perimeter fence. Whenever the wire is stretched, cut, or misaligned by an intruder an alarm is generated by a contact closure. The Israelis are generally given credit for most of the development of the taut-wire sensor. Most of the fence-disturbance sensors are subject to defeat if the intruder avoids touching the fence.

More sophisticated detection sensors have also been developed, tested, and successfully used and are commercially marketed. A microwave intrusion sensor consists of a microwave transmitter and a receiver at opposite ends of a straight section of perimeter boundary. The received

[6] In the interest of safety and for further guidance there exists an ASTM specification, designated F-792.82, entitled Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas.

[7] U.S. Congress, Office of Technology Assessment, Op. cit., footnote 1, chs. 1, 4.

Photo credit: Sandia National Laboratories, 1990.

A taut wire fence sensor.

signal is the sum of the directly transmitted signal and the signals reflected from the ground and other objects in the intervening distance. When any object, for example an intruder, moves into the stable monitored field, the microwave signal received is altered, generating an alarm. These sensors are subject to defeat by a knowledgeable intruder. This deficiency can be overcome by overlap with another sensor such as a radar or infrared sensor. Microwave sensors, like other ray-type sensors, operate across a line-of-sight, so surface grading in the clear zone between the transmitter and the receiver may be required to eliminate a blind ground depression that could create a crawl space under the microwave beam. The height and alignment of the antennas and the distance between them are important factors. Adverse environmental conditions including heavy rain, water puddles, very deep or blowing snow, windblown dust and debris, fog, vegetation, birds, and wild animals can cause nuisance alarms or malfunctions. Deep snow can obscure a careful crawling intruder. Microwave sensors are available from several suppliers.

Infrared (IR) sensors, both active and passive, are also frequently used for intruder detection. The active infrared sensor generates an alarm when the IR light beam from a transmitter, similar in many respects to that used in the common remote TV-channel changer, is broken. The transmitter and receiver are located at each end of the detection zone. Multiple infrared beams are often used, especially at gates and doors, to create a web of rays that make the system more impenetrable. Passive infrared sensors operate on the fact that all animals emit IR energy, the amount and wavelength being dependent on their body temperatures. A passive IR sensor sends an alarm when it detects a change in the incoming IR energy from its field of view, as would be generated by an intruding person. The probability of not detecting an intruder and of getting a nuisance alarm is influenced by the speed of the object, by the ambient temperature, and other environmental conditions.

A video motion detector monitors the electronic signals from a video camera and detects changes in any designated part of the video scene as would occur when an object moves within the field of view. Sometimes only a portion of the total field of view is monitored for motion. Objects other than a person, such as animals and birds, blowing debris, and snow moving through the field of view, can cause nuisance alarms. The size of the moving object or its speed (consider a flying bird) can sometimes be used to distinguish a person from other alarm objects.

In addition to the beam type sensor described above there are several other devices now commercially available for intrusion detection at a perimeter. One known as the E-field detector sounds an alarm upon the disturbance of an established electric field near a conductor. It senses changes in capacitance between the sensor elements such as wires on a fence or between fence wires and the ground. The dielectric constant of human flesh is about 100 times that of air, so as an intruder approaches an E-field fence, the capacitance changes and a resulting alarm is issued, even when the person is not yet directly between the wires. Changing weather conditions, such as humidity, cause a change in circuit characteristics, but frequently the

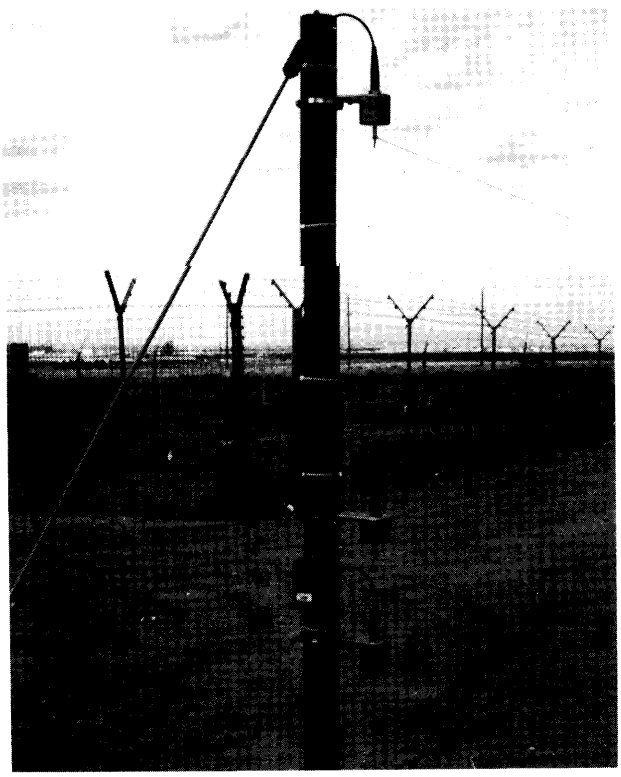
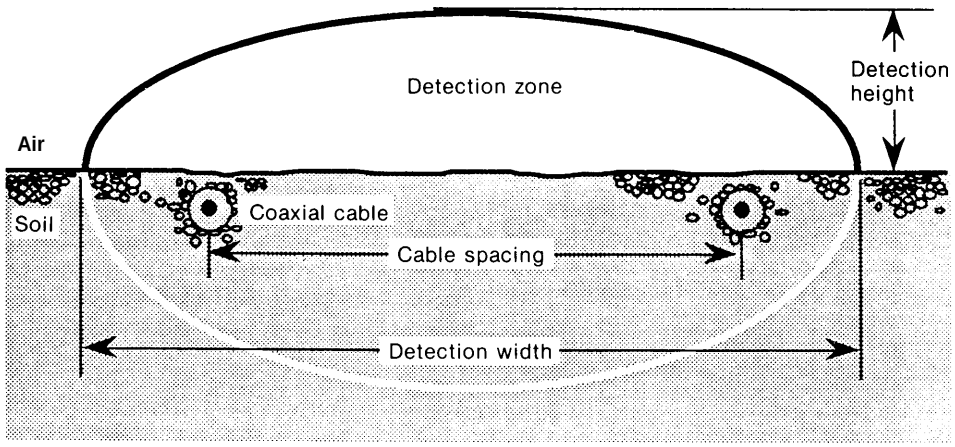


Photo credit: Sandia National Laboratories, 1990.

E-Field fence.

Figure E-2—Coaxial Cable Sensor



SOURCE: Sandia National Laboratories, 1990.

rate and size of the change can be analyzed to determine whether the change is likely to have been caused by an intruder. Unlike the beam from active sensors, the terrain along the monitored path can be crooked and irregular, providing an advantage for this type of detector. The E-field sensor is not sensitive to wind unless it carries with it snow or rain. However, the E-field sensor fence must be kept clear of moving vegetation.

Buried line **sensors are designed for intrusion detection. These sensors are usually buried in the ground for stability and protection but some are marginally suitable for stabilized temporary deployment above ground, for example around a parked aircraft or a building to be temporarily secured. Some lines are sensitive to seismic or magnetic disturbances, or both, that are transmitted through the ground to the sensing elements.**

The seismic line sensor employs transducers, which sense pressure waves from an intruder's footstep or vehicle. Piezoelectric crystals and strain gauges respond to stresses in the sensor cable due to any disturbance of the material around it. The balanced-pressure seismic sensor determines the pressure change between the two parallel segments of the buried flexible tubes caused by the added weight of a passing intruder. Another seismic-sensitive buried line responds to changes in the cable's magnetic core due to stress.

A **buried line magnetic sensor generates an electrical signal that triggers an alarm when an intruder carries or drives an object containing a magnetic material across the line. In the geophone line sensor a coil of wire is moved through a freed magnetic field by any seismic disturbance, thereby triggering an alarm.**

Disturbances that contribute to nuisance alarms are generated by animals, hail, blowing debris, nearby train **or** truck traffic, and **some** industrial noises. Nuisance alarms in magnetic sensors can also be generated by lightning or nearby unshielded power lines.

Another type of sensor consists of two coaxial cables buried in the ground about 6 inches deep and parallel **to** each other (see figure E-2). These cables are of **a conventional coaxial design except that the outer conductor is ported (made with many** closely spaced small holes through the shield). **When** electrical energy is injected **into one** cable, **some radiates out** through the cable shield and **is** coupled through the ground and the **air above the** ground **into** the nearby **receiver cable through similar small ports. When an intruder comes near one of the cables the change in coupling is** sensed and **an alarm is** generated. The sensing **zone** extends **out** about 3 feet from the cables and is effective under the cables too, so **it can** detect tunneling **as well as** aboveground activity. Surface **water from** any source, however, **is a major cause of nuisance alarms, and animals and tall plants in the vicinity of the cables can also contribute to false alarms.**

See reference 2 in the bibliography of this appendix for more detailed information about exterior intrusion detection.

Interior Sensors

A different group of sensors is available for detecting intrusion into a building that houses a protected target. Some of the intrusion sensors used at the external perimeter can also be used internally.

The widely applied balanced magnetic switch is used for indicating whether a door is open or closed and is an extension of the conventional magnetic switch used on doors and windows in home protection systems. A defeat technique is **to** place **an** overriding steel plate **(or** magnet) on the switch **to** keep the switch closed regardless of door

position. In the balanced magnetic switch system the act of adding the steel plate or the defeat magnet creates an alarm.

Sonic and vibration sensors listen and feel for intrusion indicators, such as breaking wood or glass at walls and windows, For monitoring areas like rooms during uninhabited times motion detectors are often used. Active devices for this purpose include the use of sound waves of various frequencies and beams of microwave radiation or infrared light. A very practical nonemitting (passive) infrared sensor is available that detects heat emitted from a warm object, such as a human body. An intrusion sensor that can be used very close to a target is a capacitance blanket that can be conveniently draped over a suitable target and will alarm if touched or even approached closely by an intruder.

Interior sensors are not without their vulnerabilities, which can be exploited by a knowledgeable intruder. This provides motivation for research into the operational characteristics of a sensor system prior to application. Altering power or signal lines to kill the sensor or mask its output or even interject false information is another countermeasure. Where the risk warrants, a device that monitors the line for tampering can be added.

Since commercial power sources and distribution lines are frequently vulnerable to failure due to generating equipment malfunction, storms, etc., uninterruptible electrical supplies with limited life are widely available. The size and capacity of such power supplies cover a wide range from a few cubic inches of batteries with backup energy for a few minutes to a multikilowatt diesel-electric powerplant that can be located and protected within the physical protection system.

Special design thought must be given to the routing and protection of power and signal cables to prevent exposure to adversarial attack and to protect them from ground erosion. Further, to minimize nuisance alarms, the routing of signal cables should be done so as to avoid inductive coupling with other circuits

Alarm Assessment

Alarm assessment is the next step in the security system after a sensor has detected and reported an alarm of any kind. By definition, a false alarm is caused by the malfunction of a sensor or a subsystem such as an intermittent electrical circuit or a power outage or a stray magnetic pulse (perhaps from lightning). A nuisance alarm is generated by a disturbance similar to that caused by a real intrusion but not actually generated by intruding personnel (e.g., blowing debris or animal activity). These invalid alarms, indicating intrusion activity when in fact there is none, are not only undesirable but, if frequent, are intolerable. Nuisance alarms may be eventually ignored or, worse, the offending sensor may be deliberately shut off by the irritated assessment personnel, leaving a hole in the detection system. This problem emphasizes the importance of reliability in physical protection systems. The validity of alarms in an in-depth system can frequently be determined by the simultaneous reporting of an alarm from an overlapping sensor, perhaps of a different type, detecting the same event in the same vicinity.

Closed **circuit** television is usually used for initial **assessment of an alarm. TV is usually cost-efficient in a large system since one person can monitor several areas at the same time from one central location. In addition, the TV can be ideally located and thus have a better field of view, especially with custom lighting. Personnel safety is also enhanced by the use of CCTV.**

An extensive variety of surveillance cameras is available, including the older electron tubes type and the **newer solid-state cameras each with pros and cons concerning illumination required, field of view and magnification, repositioning capabilities, power consumption, sensitivity, resolution, reliability, environmental resistance, maintenance, and cost. Additional hardware required to extend the capabilities of surveillance TV systems is available including special lenses, signal synchronizers, switches, transmission equipment, and video displays. The assessment ability of a surveillance camera is very dependent upon its mounting location and the illumination provided. The TV monitors at the central alarm and communication center are frequently operated in the standby or blank mode until an alarm is generated. They then may automatically be turned on for viewing, perhaps on a preplanned priority basis, and at the same time maps and views of the associated facility and other visual aids may be automatically brought into view to aid assessment. Another frequently used high-tech device is the alarm-triggered video recorder which can be used to provide immediate play-back of the alarm event. Recording on magnetic disc or tape or on optical disc, can be done continuously but is usually done intermittently in the interest of conserving recording media and recorder life. The TV equipment discussed above for surveillance and alarm assessment is practical, well developed, commercially available, reasonably priced, and widely used. Many suppliers are available to provide installation and maintenance information and service. Installation and maintenance is sometimes expensive, especially for retrofits.**

See references 3 and 4 in the bibliography of this appendix for supporting and additional information about intrusion **assessment and about alarm communications.**

Response Force Communication

Communication is a vital function in a physical protection system. The system most commonly used to maintain effective control and coordination of the protective force and response personnel is the popular, small, hand-held, battery-powered FAA voice radio. These radios have a range of about 1 to 3 miles, which is marginally adequate in some applications. Dead spots in the operating area are frequently experienced. The use of elevated repeaters can effectively reduce this problem. The ease with which an adversary can eavesdrop on unscrambled messages is a concern. Furthermore, deceptive messages can be injected into a radio conversation to distract and confuse the security force personnel. Message scrambling or encryption can be used to avoid this drawback. However, as a system becomes more secure, it also becomes more complex and costly and the messages become more noisy and less intelligible. Jamming, or flooding the radio transmission with noise by the adversary to make the conversation unintelligible, is also a potential vulnerability. Techniques, such as programmed frequency hopping, can be used to combat this problem. Other message-transmission media such as phone lines, intercom networks, public-address systems, and even hand signals can frequently be used as alternatives to or in conjunction with radios. See reference 5 for more detailed information about protecting security communications.

Delay Barriers

Most conventional **security** barriers **at** industrial facili**ties are** designed **to** deter **or** prevent occasional **acts of thievery or** vandalism. In the case of determined terrorist activity, however, the traditional fences, building walls, doors, locks, etc., will not prevent intrusion but each may contribute some delay. Barriers around a protected area simply slow down the adversarial penetration into the controlled area. Delay after intrusion detection contributes to the time needed for response-force notification, deployment, and action. Each additional second required by the adversary after detection provides that much more time for the security response force to interrupt the terrorist action. It should be emphasized that if the adversarial action is not detected early in the penetration attempt, barriers will be much less effective.

Tests have shown that some barriers which appear to be impenetrable can be breached quite rapidly by determined terrorists who are trained and well equipped. In keeping with the theme of protection-in-depth, the use of several different kinds of barriers may demand of the adversary more penetration equipment, a larger team, more transportation equipment, and more penetration time. If the imperviousness of a barrier (or the perception thereof) is sufficient to deter or prevent the attack, it has accomplished its purpose.

Large protected **sites** occasionally include **natural** barriers such **as rugged coastlines,** high cliffs, **mountains, or** long, clear **distances. Most** barriers, however, **must be constructed and installed.**

Perimeter Barriers

Perimeter barriers form the outermost elements of most physical protection systems. The most common type of outer perimeter is the chain-link fence. Security fences are usually about 8 feet tall and have extension arms angled upward at the top with several strands of barbed wire and are sometimes also topped with a roll of concertina (entanglement barbed wire). If appropriate, the lower edge of the fence can be buried deep enough to discourage shallow tunneling. Although chain-link fences may serve as a deterrent to the casual intruder, most industrial perimeter fences can be scaled or penetrated with handtools very quickly and they do not delay determined adversaries for more than a few seconds. Common handtools (manual and power), thermal cutting tools, explosives, and ram vehicles are the favorites for penetrating barriers. However, if one or several rolls of barbed wire or razor tape are placed on or near a perimeter fence, penetration can be made more difficult in some cases and more time consuming. Several configurations of barbed wire and razor tape, usually in rolls, have been developed and tested for delay efficiency. Some razor tapes have built-in sensors to detect cutting, thus making penetration without detection more difficult.

Much characteristic information regarding perimeter barriers of all types, including the approximate times to defeat have been determined from penetration tests. This sensitive information regarding effectiveness about many kinds of imposing barriers can be found in reference 6 in this appendix's bibliography and can be used for design and operational purposes.

Several lethal barriers, such as electrified fences and fields of explosive mines, have been considered as perimeter barriers, but many problems are involved in the installation, maintenance, safety, and legality of lethal barriers and they are seldom used except for high-risk military installations.

Vehicle Barriers

Personnel barriers are usually ineffective against even small vehicles such as cars and pickup trucks, so specially designed vehicle barriers must be erected where the threat of ramming is sufficiently high. There are many kinds of vehicle barriers to choose from, such as earthen ditches and banks and other fixed barriers (e.g., filled steel tubes), movable heavy concrete (e.g., ''Jersey bounce blocks' or heavy earth-filled concrete planters), and convertible barriers like the pop-up wedge. Loaded trucks and rail cars are sometimes used for quickly obtainable temporary barriers. Large, half-buried tires make reasonably effec-

tive barriers for some applications. An alternate to ramming a barrier is bridging it. Bridging may be especially applicable for excavated, earthen, and other low-level barriers. A motorcycle may be used by the adversary especially if the intrusion and escape equipment can be carried on such a vehicle and if the other onsite vehicle restrictions are designed against only larger vehicles.

The concrete Jersey bounce and conventional highway guardrail cost about $40 per foot installed. Half-buried, large tires cost about $5 per foot installed.

Barriers On Buildings

Doors and windows are logical points of attack. Attack methods for these portals include the use of manual and power handtools, oxygen-fed burn bars, explosives, and ramming vehicles. Attack-resistant windows and doors, doorframes, hinges, and locks are available for secure buildings at increased cost. A full-height turnstile is the functional equivalent of a security door and is generally subject to the same kinds of attacks. Other openings such as ventilation ducts, large water pipes, and other utility ports are also vulnerable points and must be considered.

Walls of buildings, vaults, and other structure are usually considered to be more resistant to penetration and less attractive as targets for forced entry than are doors, windows, air vents, and other conventional openings.

Because of their structural reputation and rugged appearance, concrete walls are almost universally believed to be formidable barriers. However, in conventional construction, the kind and shape of the concrete and the size and spacing of reinforcing bars are located for structural requirements and not to prevent penetration. Testing has shown that standard reinforced concrete walls are vulnerable to rapid penetration.

Explosives are especially effective against concrete walls. The shock waves produced by an explosion propagate through the concrete and result in fragmentation and spalling. The fragments are forced out, leaving a relatively clean hole except for the rebar, which often requires more time to remove than the concrete. The use of precast T-section walls or roofs generally provides little delay because of the lack of rebar. A technology for security walls, not usually used for conventional construction, includes the use of special aggregate ingredients such as steel wires or balls of ceramic or lead to provide more resistance to penetration by using cutting and burning tools or explosives. The use of a stand-off wall, located a few inches ahead of the main protection wall, requires added time for its removal or requires the use of a much larger or a second explosive charge. These supplementary features add cost to the protective structure.

One advantage of concrete barriers, even if penetration time is less than might be expected, is the sophistication and weight of tools that must be carried by the adversary.

Vaults

A vault is considered hereto be a strong repository the size of a small room, usually within a larger building. It is constructed to secure its content from unauthorized persons and is usually not a workplace. With the right equipment, the time required to penetrate an 8-inch reinforced-concrete vault wall and a half-inch steel door is only a few minutes. Earthen overburden when appropriate, can add appreciable time and adversary exposure to the breaching process, depending on its thickness and the removal equipment used. New facilities requiring heavy physical protection might appropriately be totally buried. Although subterranean construction is not frequently used, the technology and basic design considerations have been well established. The comparative cost range per square foot of several wall materials in place is about $15 for 1 inch of steel, $8 for 10 inches of conventional concrete, $40 for expanded metal/concrete (the kind frequently used in safe-deposit vaults), and $0.50 for 30 inches of soil overburden often used on the top of large vaults.

Dispensable Barriers

Barriers may be passive, like walls and fences, or active and quickly dispensed into place. Dispensable barriers and deterrents are designed to add physical encumbrances and to interfere with an adversary's personal sensory and motor processes. Such barriers include rapidly dispensable rigid foams, sticky foams, aqueous foams, sticky sprays, slippery sprays, sand columns, noise, lights, smoke, and rubble piles. Most of these materials can be stored in a compact form in an out-of-the-way place and dispensed quickly when sufficient threat warrants. This dispensable denial technology augments the usual protective structures. If such items are used, the adversary must conduct his breaching activities, which now may be more taxing or hazardous, while in personal protective gear further reducing his speed and endurance.

Obscurant materials include smoke of various kinds and aqueous foams. Techniques for generating obscuring and irritating smokes are quite well known from military literature.

Psychological stresses, such as flashing lights at various frequencies and intensities, are believed to be of little deterrent value. Likewise, the use of sound at very high and very low frequencies is not considered to be an effective adversarial deterrent. However, high-intensity audible sound, besides being very uncomfortable to the unprotected ear, makes audible communication between adversary team members very difficult, adding more time to the barrier breakthrough task. The cost of such a noise

generator is quite minimal. A very high-intensity continuous light (above 1 million candle power) has been determined by Navy security organizations to be effective in temporarily blinding an adversary and thus causing delay.

Polyurethane is a popular rigid foam that can be expanded to 30 times its stored volume. It can be used on short notice to block a passageway or sometimes directly to encapsulate a protected item. Many formulations of polyurethane foams for this purpose are commercially available and cost about $50 per cubic meter of foamed volume. The dispensing equipment costs about $5,000 to $10,000. There are hazards to a person caught in the foaming process such as entombment, exposure to 130 'C temperature, and possible chemical toxicity.

Sticky foam has an expansion ratio of about 30 to 1 for the frost few hours. It effectively entangles the adversary and fouls his equipment. When appropriate, it may even be applied to the target. The foam costs about $50 per cubic meter dispensed. Similarly, sticky spray, with little expansion, is intended to be applied on command with entangling effects similar to sticky foam. These sticky materials are very effective mechanical impediments. However, as one might imagine, the clean up operation after dispensing the sticky stuff is laborious and expensive.

Slippery materials greatly reduce normal friction on smooth walkways and equipment, making the terrorists' progress slower and more hazardous. The material is applied in dry powder form but when sprayed with water becomes an "instant banana peel."

An airborne obscurant can render the adversary "blind" and slow his progress by making it difficult for him to recognize targets, tools, team members, and entanglements. Several smokes and smoke generators are now commercially available. Smoke generators cost from about $25 for a single military smokepot to a more exotic and much faster system for about $10,000.

Aqueous foam is generated by spraying a detergent-like surfactant solution onto a screen while blowing air through the screen, resulting in a material expansion factor of from 100 to 1,000. A dispenser that makes about 100 cubic meters of soapsuds-like foam per minute costs about $2,000. This foam is also a fire suppressant and can absorb significant energy from an explosion, which may be of some interest. About the only hazard to personnel is becoming sufficiently covered so that the person can no longer breathe.

Sensory irritants, such as tear gas, respiratory irritants, and some pain-producing agents, quickly produce an incapacitating effect once in contact with the skin, eyes, and nose. Distress symptoms soon disappear when exposed to fresh air. The large margin between incapacitation and lethality makes some substances, such as "CS" and "CR," agents of choice.

The social acceptance of dispensable deterrents and the related legal aspects must be considered in determining their applications.

Physical protection systems range in size from one building with a few protection features to a multi-acre site with the full array of entry control, detection, assessment, delay, and response systems and the appropriate security and operating personnel.

Response Force

The last element of a physical protection system is the response force, made up of trained security personnel, and the necessary equipment, such as weapons, body protection, transportation, communication, etc. Clearly, a physical protection system without a response force would be of little use in many applications (although for some situations, the eventual response force may be local law enforcement personnel not actively involved in the site security plan). An intrusion alarm would get little response and any barrier, however formidable, would be eventually surmountable with no opposition. The purpose of the response force is to intercept and neutralize the intruding adversary.

A part or all of the response force may be located on-site or off-site. The response force maybe made up of local or State police, military force, a dedicated response team, or some combination thereof, which mayor may not include regular security system operating personnel. Because of the variety of response-force compositions, it is difficult to generalize about specific procedures and tasks that the force may be expected to perform but the final objective is clearly to prevent the adversary from accomplishing his objective.

Accurate and timely communications with the response force must contain as much information as possible about the adversary force size, actions, tools, weapons, location, direction, etc., and instruction for response-force deployment. Aside from the personal safety of the individuals, it is clear that the response force must survive intact and so must be trained in tactics for the safety of its personnel. Training includes instruction about the facility's corridors for cover and concealment and to avoid ambush. A computer-based technique known as surrogate travel is available to aid in deployment and tactical movement. Tactical practice is necessary for response-force proficiency and will provide realistic estimates of response times and tactical plan validity.

A group of firearms that project laser beams has been developed. When used with jackets and helmets that detect the laser light, response training may be devised with little risk to the trainees. These devices for shooting

"laser bullets' are commercially available in the form of handguns, rifles, submachine guns, and other weapons.

To ensure adversary neutralization in the most time-effective manner, a balance is necessary among the several response-force constituents, including the number of force personnel, planning, training and practice, and the available equipment. Members of the response force must have rapid access to the needed weapons, vehicles, radios, and personal protection equipment (i.e., body armor, helmet, protective clothing, and sometimes gas masks and contained breathing equipment), all consistent with the environment and the expected conflict. The equipment required for the response force is strongly dependent on the other characteristics of the physical protection system.

Construction Technologies and Strategies

Above, a number of technologies have been presented that help protect fixed sites against unauthorized entry. These fell into three broad categories: perimeter barriers, sensors and alarms, and access control. In addition to these fields, there is the important area of architecture and engineering applied to buildings that may become targets of attacks. The primary threat discussed below is bombing, perhaps the most common and certainly the most deadly tactic used by terrorists against U.S. diplomatic installations and military installations.

Obviously, it is far easier to implement protective measures by incorporating them into the design of a facility *before* **it is built, rather than to retrofit fixes after the fact. However, there exist options for reducing vulnerability to attack with explosives even in the latter case. Most of the technical aspects that follow are not "high tech," but, rather, are in the domain of classic civil engineering and architecture. What follows is a brief survey of a developing field.**

Bombs may be introduced into a site by brute force (e.g., a vehicle bomb), by throwing or launching, or by stealth (e.g., inside mail). The first tactic is the most difficult to defend against, since a very large quantity of high explosive (several tonnes) may be used. If this threat is successfully opposed, lesser tactics, such as throwing a bomb over a wall, can be dealt with relatively easily. To put the matter in perspective, the amount of explosive needed to destroy an aircraft is on the order of hundreds or thousands of grams; a tonne is a million grams. Car and truck bombs, made of up to a tonne or two of dynamite or plastic explosive, have been commonly used across the world, from Beirut (against the U.S. Marine Barracks and against diplomatic buildings), to Belfast, to Bogota, Colombia. They are able to cause the collapse of multistory buildings made of reinforced concrete, even when the bomb is located tens of meters from the target.

The design response to such a threat incorporates several elements. The first relies on enforcing a standoff distance around the potential target.[8] The standoff distance will depend on the size of the threat and on the inherent resistance of the building to overpressure. Only carefully screened vehicles would be allowed within this distance from the target. For some purposes, a 150-foot (about 45-meter) distance is used. Clearly, for retrofitting existing buildings, it is usually impossible to satisfy this requirement. However, the requirement can often be met when starting from scratch, that is, before site acquisition and design are completed for a new building.

Another layer of defense against vehicular bombs is the use of barriers and of layout and landscaping. The strength of the barriers is determined from the speed and the weight of the postulated threat vehicles. The energy that needs to be "absorbed" in order to stop a vehicle attempting to traverse a barrier is proportional to its weight (strictly speaking, to its mass) and to the square of its Speed.[9] Some types of barriers have been mentioned in the previous section (e.g., the Jersey Bounce blocks); there are others, ranging from large reinforced "flower pots' to concrete-filled cylinders, pyramids, cubes, tires, and 55-gallon drums. Stopping power for each in terms of vehicle speed and mass can be calculated and tested. Some barriers are active, rather than passive; normally not deployed, they can be rapidly activated in case of alarm. A familiar version is the drum type, which, when dormant, is flat, allowing easy passage. When activated, a plate, supported by a heavy cylinder, rapidly rotates upward from the ground to block a vehicle. In addition, one might place ditches or earthen berms in strategic places around a target building. The ditches would cause trucks to tip down if they attempt **to cross; any** blast would then be partially broken **by the ditch. Berms also function to break the path of the blast wave through the air.**

In order to reduce the speed to which vehicles may accelerate, barriers and obstacles may be laid out along access roads. Right angle turns, S-curves, traffic circles, movable barriers, are all options to this end. Maximum speed at turns are determinable from the turn radius; likewise, the maximum speed achievable between barriers (from a dead start) can be easily determined in planning traffic layouts.

In designing a building that maybe a target, both the layout and the strength of individual elements must be calculated. Those areas containing critical facilities

[8] **This discussion of protection against bombing attacks against fixed site facilities relies largely on** information from U.S. **Army Corps of** Engineers, *Security Engineering Manual (Official* Use Only), **Protective Design Center, Missouri River Division-Omaha** District (Omaha, NE: U.S. Army Corps of Engineers, January 1990).

[9] **The kinetic energy of a** moving object is one-half the product of its mass and **its speed squared.**

should be placed towards the interior of the structure. Corridors and less essential rooms may be placed as buffers around the more critical areas. Windows in exterior walls provide a clear vulnerability; it is preferable to place windows around an interior courtyard.

Exterior walls should be designed to resist blast effects, given the standoff distance and the quantity of explosive taken to be the credible threat. For engineering design, tables have been calculated showing, e.g., the protection levels afforded against a 1,000 pound high explosive by reinforced concrete walls of various thicknesses, as a function of the standoff distance. Similar analyses are available for blast resistance in doors and windows. Roofs should be designed of reinforced concrete with a maximum span of 1.5 times the supporting wall spans. The thickness of roof slabs can be determined from similar tables that provide the blast resistance as a function of thickness and stand-off distance. Additional safety measures to take include using shatterproof lenses on light fixtures and bracing suspended fixtures, ductwork and plumbing.

The structural framing system should be able to resist forces and torques applied when the building suffers the blast load. Exterior exposed columns must be hardened to withstand blast effects. The framing structure should be designed to avoid a concatenation of failures, in case of failure of an element. This criterion must be incorporated to avoid catastrophic collapse of the entire building under blast load.

The above discussion can be amplified by tables from reference 1. Technical experts present, in addition, abroad set of design features to avoid, such as long spans, prestressed load-bearing cables, masonry buildings, and bar joists. Implementation of the blast-resistant features provides protection similar to hardening buildings against earthquakes.

Appendix E Bibliography:

1. **"Entry-Control Systems Technology Transfer Manual," SAND87-1927 (Albuquerque, NM: Sandia National Laboratories, May 1989).**
2. **"Exterior Intrusion Detection Systems Technology Transfer Manual," SAND89-1923.UC-515 (Albuquerque, NM: Sandia National Laboratories, May 1990).**
3. **"Video Assessment Technology Transfer Manual," SAND89-1924.UC-515 (Albuquerque, NM: Sandia National Laboratories, October 1989).**
4. **"Alarm Communications and Display Technology Transfer Manual, " SAND90-0729.UC-515 (Albuquerque, NM: Sandia National Laboratories, November 1990).**
5. **"Protecting Security Communications Technology Transfer Manual," SAND90-0397.UC-515 (Albuquerque, NM: Sandia National Laboratories, March 1990).**
6. **"Access Delay Technology Transfer Manual," classified UCNI, SAND87-1926/l .UC-5 15 (Albuquerque, NM: Sandia National Laboratories, September 1989).**

All the above documents may be obtained from Director, Office of Safeguards and Security, U.S. Department of Energy, on a need-to-know basis.