Chapter 1

Summary

Contents

Page

INTRODUCTION 4
OUTLINE OF REPORT 4
FINDINGS 5
Chemical and Biological Terrorism 5
Interagency Communication and Coordination 6
Options 7
Aviation Security 8
Integrated Security Systems 9
Human Factors 10
FAA Research and Development Program 11

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.