Chapter 4

Research and Development

INTRODUCTION

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

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

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

Explosives Detection

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

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

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

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

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

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

baggage inspection on airlines, dogs are not appropriate.

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

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

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

Chemical and Biological Agents

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

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

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

Physical Protection

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

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

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

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

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

Incident Response

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

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

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

Data Dissemination

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

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

DETECTING EXPLOSIVES

Introduction

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

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

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

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

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

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

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

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

The Explosive Threat

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

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

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

History

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

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

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

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

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

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

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

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

Table 4-l—Some Common Explosives[a]

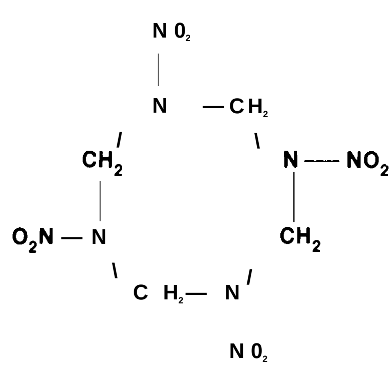
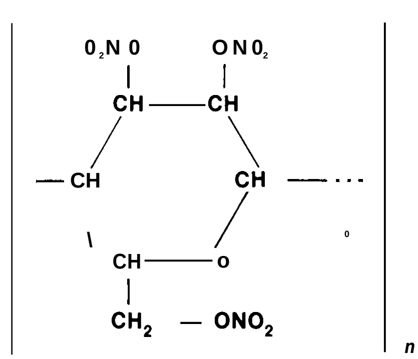
TRADE OF POPULAR NAME(S)	CHEMICAL NAME, FORMULA, AND STRUCTURE	COMMENTS
AN, Ammo-Nite	Ammonium nitrate $(NH_4)^+ (NO_3)^-$	Also commonly used as a fertilizer. Frequently mixed with fuel oil to make explosive called ANFO.
Black powder		Mixture of potassium or sodium nitrate, sulfur, and charcoal. Explosive most commonly used in terrorist bombs in the United States.
Composition B		60:40:1 mixture of RDX:TNT:wax
Dynamite		Compositions have varied over the years. The explosive components of modern dynamites are principally EGDN and NG absorbed onto combustible pulp (e.g., wood meal, starch, rye f l our),
EGDN	Ethylene glycol dinitrate H_2C-ONO_2 H_2C-ON0_2	One of the main components of dynamite. Quite volatile, making detection by “sniffers” relatively easy.
HMX, Octogen	Cyclotetra-methylene tetranitramine; 1,3,5,7-Tetranit ro-1 ,3,5,7-tetrazacyclooctane 	A military plastic explosive.
Nitrocellulose, gun cotton[b]		Main component of smokeless powder.

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

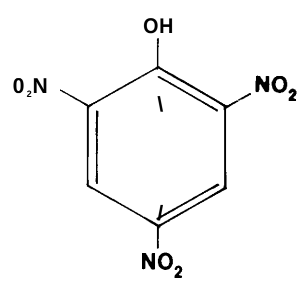
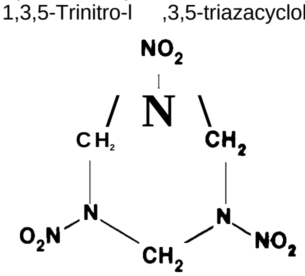
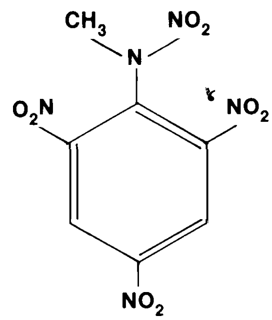
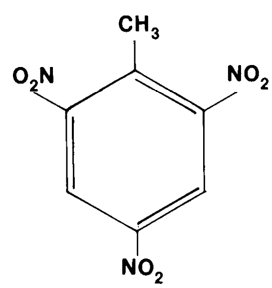
NG Nitroglycerine	Glycerol trinitrate H_2C-ONO_2 H! $CONO_2$ H_2C-ON0_2	
PETN	Pentaerythritol tetranitrate CH_2ONO_2 | 0_2NOCH_2— C- CH_2ONO_2 | CH_2ONO_2	A plastic explosive available in bulk form or, with modifications, in sheet form under tradename “Detasheet.” Unusually low nitrogen density for a plastic explosive: 18 percent by weight (compare with RDX).
Picric Acid	Trinitrophenol 	
RDX, Research Division X, Formula X, Cyclonite Hexogen	Cyclotrimethylenetrinitramine; 1,3,5-Trinitro-l ,3,5-triazacyclohexane 	Primary ingredient of military plastic explosives known as C-3 and C-4. 38 percent nitrogen by weight.
SEMTEX		A Czechoslovakian-made explosive composed of a mixture of varying proportions of RDX and PETN along with binder and plasticizer.

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

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

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

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

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

Methods of Explosives Detection

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

Table 4-2—Explosives Detection Technologies

Bulk detectors:
Using ionizing radiation
Nuclear
—Thermal Neutron Analysis
—Fast Neutron Analysis
—Nuclear Resonance Absorption of Gamma Rays
—Associated Particle Production
—Pulsed Fast Neutron Analysis
—Pulsed Fast Neutron Backscatter
-Nitrogen-1 3 Production with Positron Emission Tomography
X-ray
—Transmission
-Backscatter
—Dual- or Multi-Energy
-Computerized Tomography
Using non-ionizing radiation
Nuclear Magnetic Resonance
Electron Spin Resonance
Nuclear Quadrupole Resonance
Vapor or residue detectors:
Dogs
Gas Chromatography (GC)/Chemiluminescence
GC/Electron Capture
Ion Mobility Spectrometry
Mass Spectrometry (two-stage)
Bioluminescence

SOURCE: Office of Technology Assessment, 1991.

The characteristics generally common to explosive compounds are:

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

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

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

Nuclear Methods of Explosives Detection

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

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

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

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

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

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

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

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

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

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

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

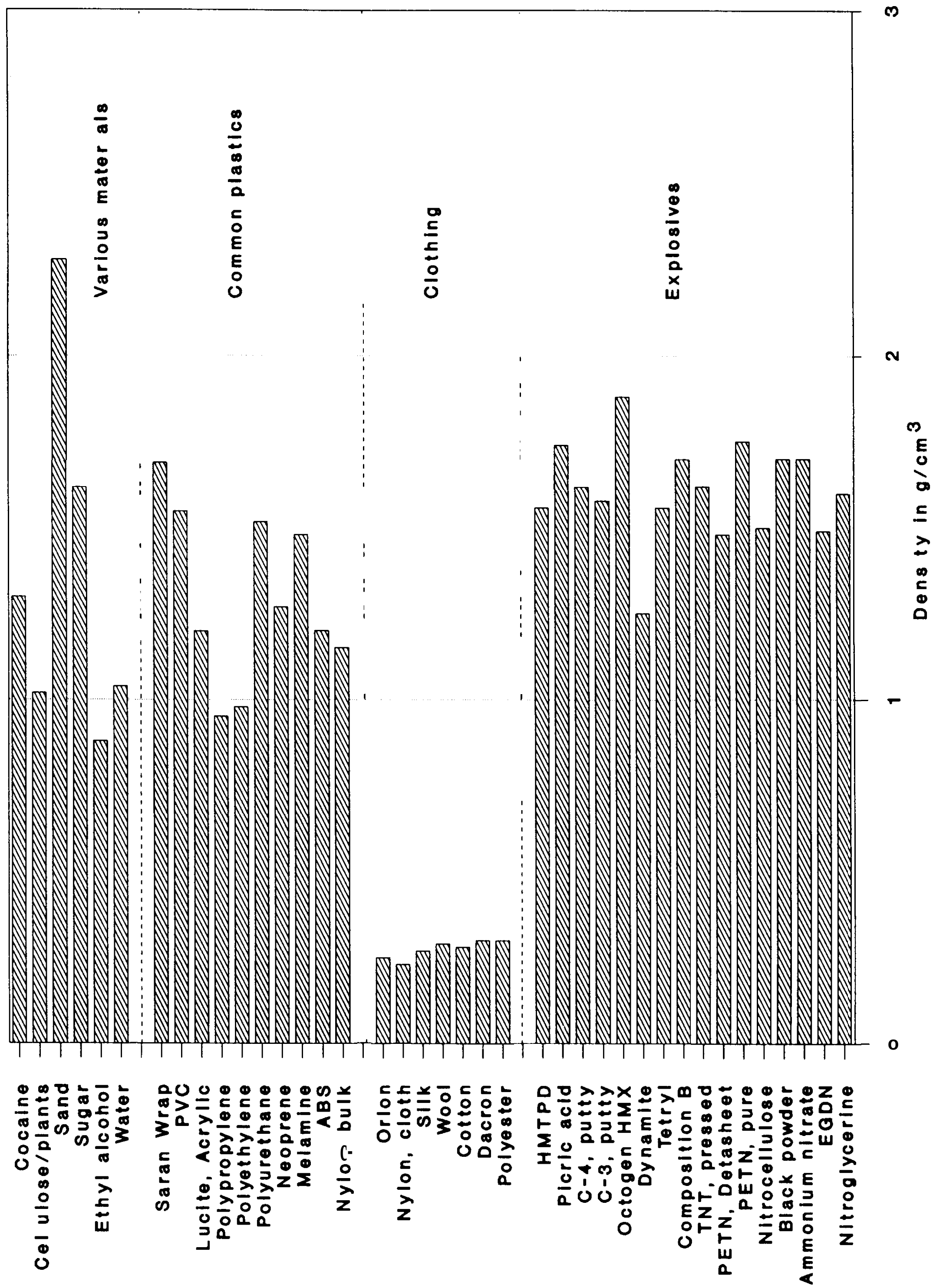
The numbers for detection probability and false-alarm rate vary, depending on several alternative details of the integrated detection system. Adding an x-ray device to TNA (utilizing and correlating information from both systems) and retrying suspect bags both change performance. Performance also varies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

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

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

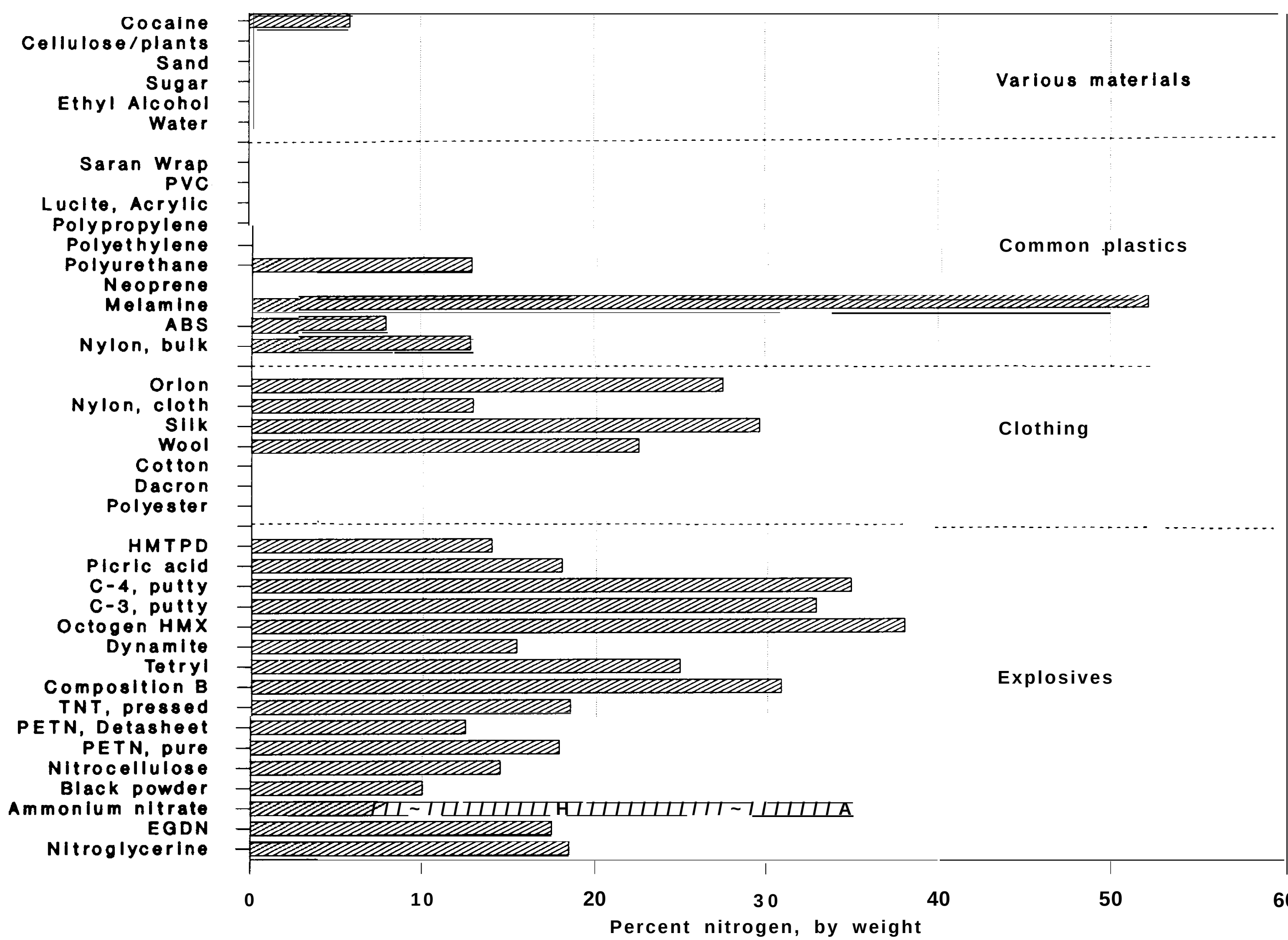
Beyond TNA, there are a number of nuclear-based systems that are in the laboratory demonstration stage. Several hold the promise of improving on some of TNA's shortcomings. One avenue of approach is to use faster neutrons, which allows the detection of elements other than nitrogen, such as oxygen and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

Figure 4-1—Densities of Various Materials



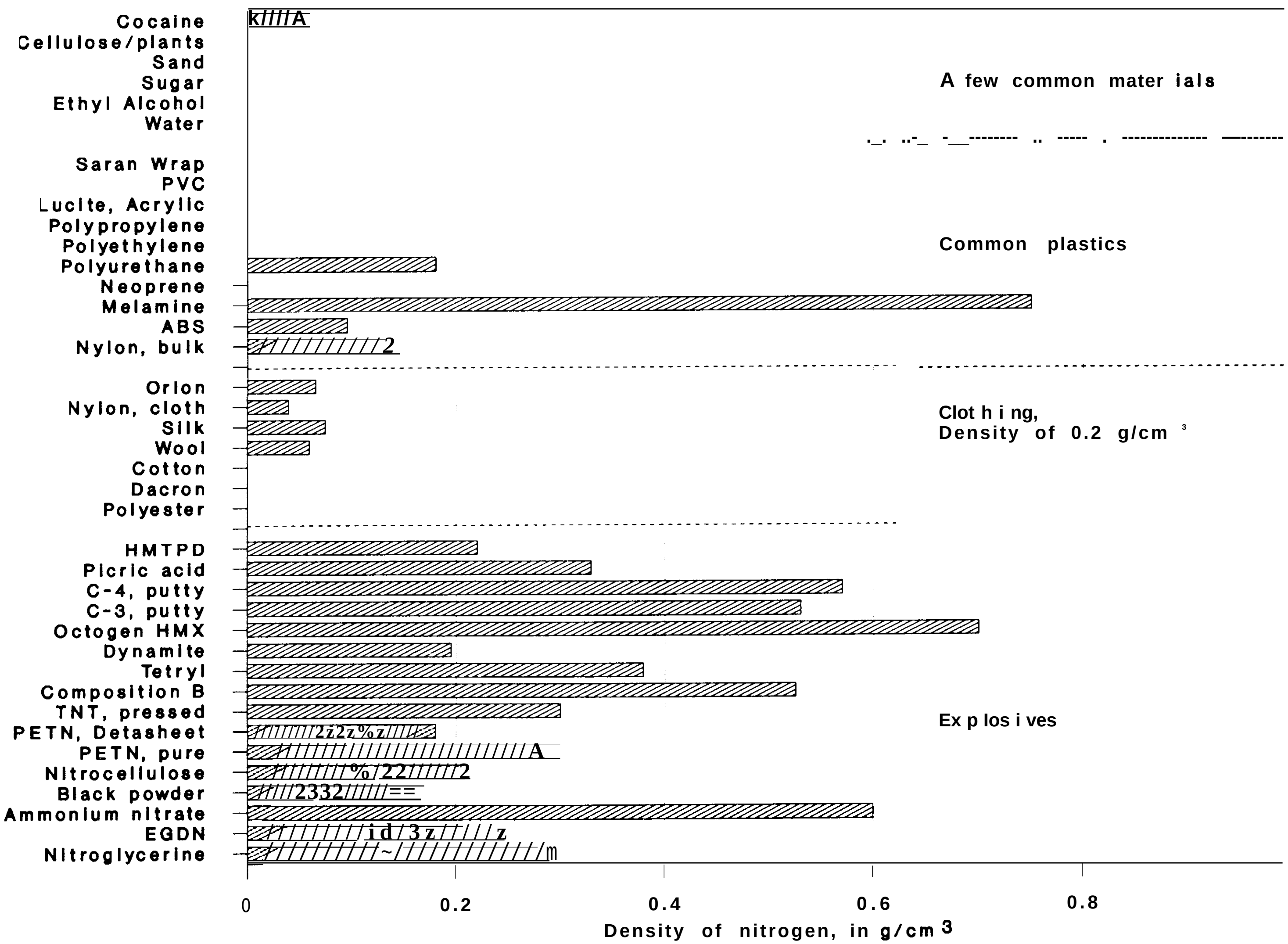
SOURCE: L. Grodzins, 1990.

Figure 4-2—Nitrogen Percentage of Various Materials



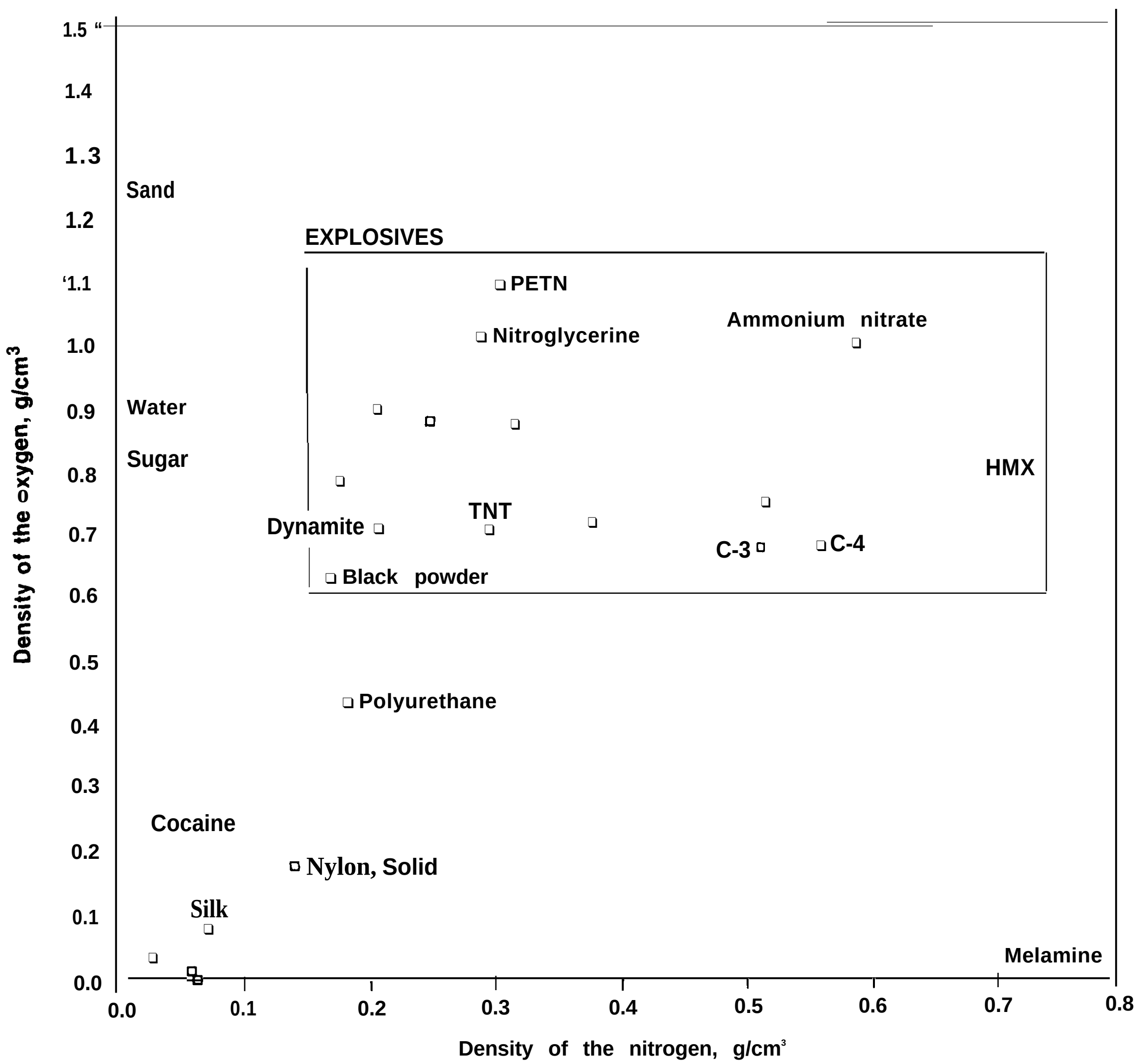
SOURCE: L. Grodzins, 1990.

Figure 4-3—Nitrogen Density of Various Materials



SOURCE: L. Grodzins, 1990.

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



SOURCE: L. Grodzins, 1990,

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

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

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

Accelerator Technology

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

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

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

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

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

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

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

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

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

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

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

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

X-Ray Technologies

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

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

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

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

Explosives Detection by Magnetic Resonance and Nuclear Quadruple Resonance

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

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

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

Vapor Detection by Chemical Means

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

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

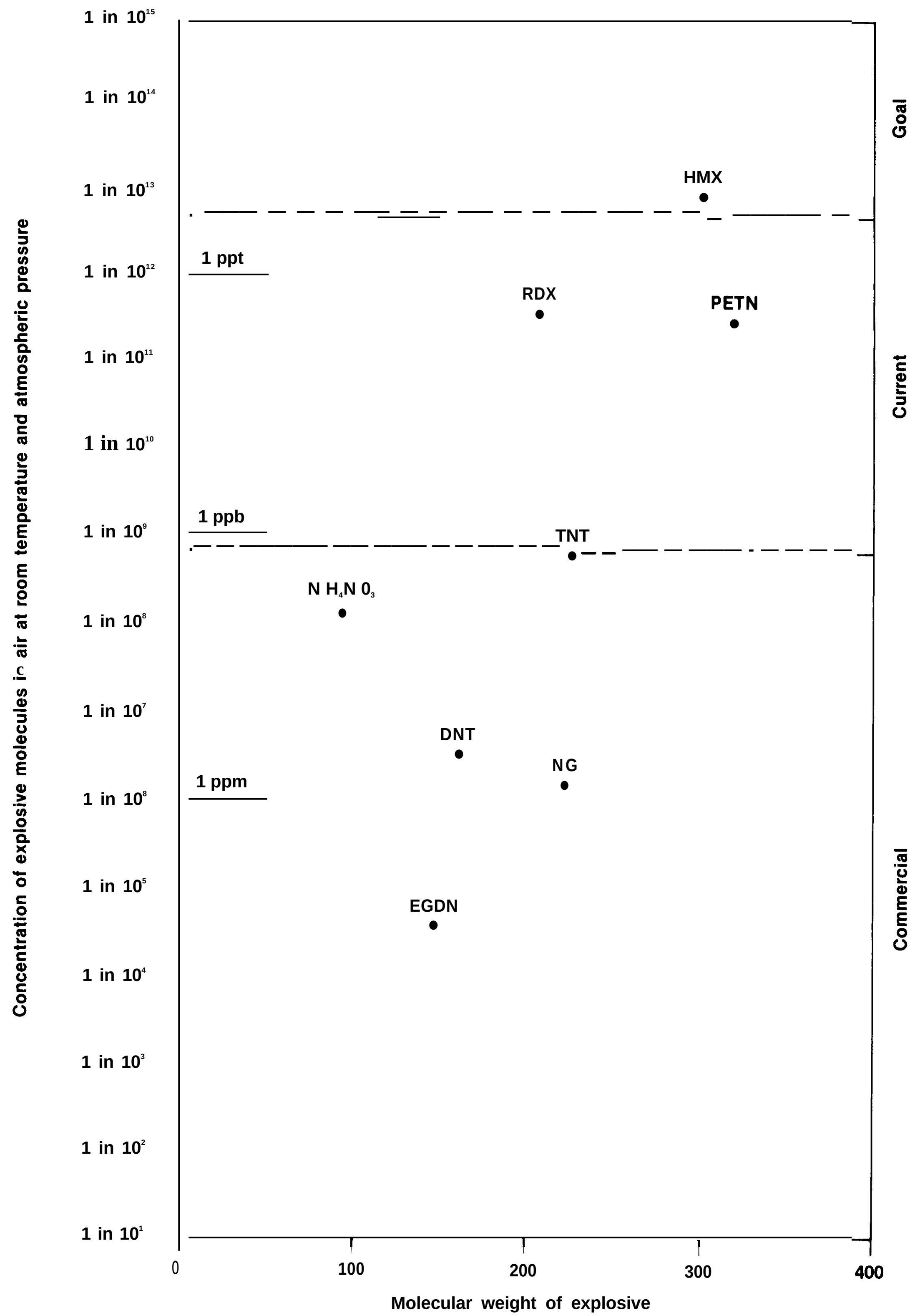
A saturated vapor of DNT (dinitrotoluene, a common contaminant in TNT--trinitrotoluene) or nitroglycerine (NG) will contain about one molecule of target compound per million molecules of diluent. Ammonium nitrate (AN) and TNT itself will be present at a concentration of about 1 part in 100 million (108). The plastic explosives RDX and PETN are even less volatile, being present in a saturated volume of air at standard temperature and pressure at a concentration of one part in one million million (or trillion—1012). This concentration is comparable to one shot glass of whiskey in Loch Ness, about 30 cents out of the national debt or 1 second out of 32,000 years.[12] HMX is, by a factor of about 60, even less volatile. These concentrations represent saturation, a condition unlikely to be encountered in the field. Thus, in all likelihood, substantially less material than suggested here will be available for capture.

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

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

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

Figure 4-5-Relative Volatilities of Some Common Explosives



SOURCE: Sandia National Laboratories, 1990.

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

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

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

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

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

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

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

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

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

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

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

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

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

Taggants

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

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

---

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

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

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

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

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

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

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

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

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

DEFENSE AGAINST CHEMICAL AND BIOLOGICAL WARFARE (CBW) AGENTS

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

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

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

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

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

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

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

Table 4-4 gives some typical detection goals set by the U.S. Army for several of the most common chemical and biological agents envisioned as possible threats. The quantities cited give an idea of their effectiveness. United Nations experts have estimated that a person drinking 100 milliliters (less than a half cup) of untreated water from a 5 million liter reservoir would become severely sick and perhaps die if the reservoir had been contaminated by 1/2 kg of Salmonella typhi (the causative organism of typhoid fever), 5 kg of botulinum toxin (a plausible toxin warfare agent), or 7 kg of staphylococcal toxin (another plausible warfare toxin). By contrast, it would require 10 tons of potassium cyanide (a chemical warfare agent) to contaminate the reservoir to the same toxicity.

Chemical and Biological Agents—Point and Remote Detection

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

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

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

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

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

Table 4-4-Chemical and Biological Agent Detection Goals

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

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

SOURCE: U.S. Army, 1990.

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

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

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

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

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

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

PHYSICAL PROTECTION

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

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

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

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

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

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

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

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

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

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

Detectors and Alarms

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

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

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

Barriers

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

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

Building Hardening

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

Aircraft Hardening

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

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

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

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

Access Control

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

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

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

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

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

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

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

Baltimore-Washington International (BWI) Airport Project

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

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

[19] 14 CFR 107.13, FAA Regulations.

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

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

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

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

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

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

INCIDENT RESPONSE

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

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

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

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

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

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

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

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

DATA DISSEMINATION

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

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

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

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

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

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

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

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