Chapter 2
Introduction

THE ROLE OF TECHNOLOGY IN COUNTERING TERRORISM

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

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

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

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

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

OUTLINE OF THIS STUDY

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

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

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

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

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

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

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

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

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

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

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

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

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

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