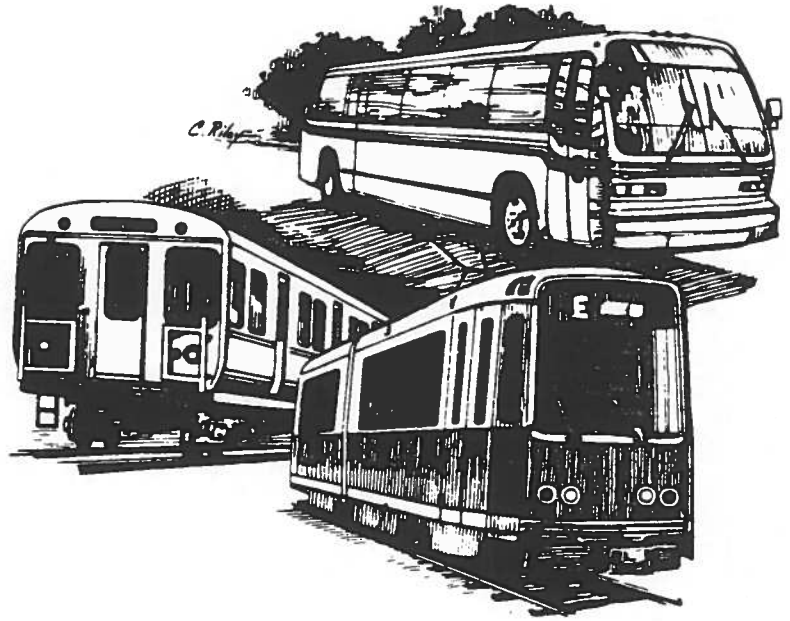# STUDY ON
TRANSIT TERRORISM

Prepared for:

U.S. Department of Transportation

URBAN MASS
TRANSPORTATION
ADMINISTRATION

Transportation Systems Center
Cambridge, MA

Prepared by:

Mr. Richard E. Clement

Counterterrorism and Security Technology

and

Advanced Technology, Inc.

Order Number DTRS57-86-P-81186

EXECUTIVE SUMMARY

This study was performed for the Department of Transportation's Urban Mass Transportation Administration under a purchase order issued by the Transportation Systems Center (TSC). It addresses requirements for improving security in U.S. urban mass transit systems in light of increased terrorist threats. The study's aims were intended to highlight areas where changes are needed to more clearly define the threat of terrorism, to make better use of available resources to protect what could become an inviting target for terrorist attack, and to develop a methodology to identify vulnerability in existing mass transit systems. The study involved in the collection and analysis of information provided by the Urban Mass Transportation Administration, acquired in interviews with officials of mass transit systems, and obtained from material in the public sector.

The study found that safety and security problems have not been well identified and that when competing for limited resources, it is difficult for mass transit systems to sustain ongoing programs for drills and simulations to maintain good levels of counterterrorism readiness. Even the programs which do exist do not preclude wanton terrorist attacks. To make matters worse, transit systems are not only unprepared against attacks, but most cannot rapidly enlist assistance from law enforcement resources specifically directed toward counterterrorism. There is a reluctance on the part of local authorities to allow federal intervention and a lack of clear distinction between criminal and terrorist actions. As a result, a transit system may not receive advance warning of an increased threat against its passengers and assets; and federal, state, or local officials may not become aware of a particular terrorist pattern until it becomes a major problem.

One of the first issues that must be addressed is the need for a universal determination of what constitutes terrorism, a terrorist incident, and a prevented terrorist incident.

The following definitions are the minimum criteria used by the FBI to determine whether criminal acts should be labeled "terrorist":

<u>"Terrorism:</u>

"Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

.

<u>"Terrorist Incident:</u>

"A terrorist incident is a violent act or an act dangerous to human life in violation of the criminal laws of the United States or of any state to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

<u>"Terrorist Incident Prevented:</u>

"A documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity."

In order to give a clearer picture of trends and dimensions of the terrorist problem in the United States, this report includes a section on terrorist-related activities; i.e., criminal acts committed in support of or as a result of terrorism but not intended to intimidate or coerce in furtherance of political or social objectives. A bank robbery committed for the purpose of financing a terrorist group is an example of a terrorist-related activity that falls short of meeting the incident criterion.

Acceptance of these definitions will allow a counterterrorist response to proceed while the fact that the incident is a terrorist act is still being established. In this way, a local authority can call on fully trained and properly equipped counterterrorist law enforcement officials without delay, in hopes of forestalling the implementation of the terrorist act.

The next area for improvement, the ability of transit systems to respond to a terrorist threat through the sharing of intelligence information on a possible terrorist activity or preparations for such an activity. Current local and federal reporting requirements are not exacting enough to reveal unannounced or unclaimed terrorist acts.

A series of preliminary terrorist acts of sabotage could go unnoticed as unconnected equipment failures even though examination of available information would clearly indicate a pattern. There is currently no means to collect this information on a detailed and timely basis. A routine review of mass transit system failures and accidents with an eye toward terrorist patterns could provide early warning of a threat if data were compiled quickly in a system that possibly incorporated artificial intelligence techniques.

The threats to and vulnerabilities of transit systems across the country vary greatly. Recent analysis of FBI-recognized terrorist acts have shown that no connection has yet been found to link these activities to a sovereign foreign state. There were recent reports of groups of U.S. criminals who solicited funds from foreign governments to undertake terrorist activity, but no government responded to these offers, and the groups were apprehended. The motivations most prevalent for committing such acts have been family arguments, disputes with former employers, and the goals of self-proclaimed, U.S. based revolutionaries who have financed their operations through other criminal acts such as armed hold-ups and extortion.

Finally, there is the question of how funding should be allocated if it becomes available. To begin to determine the greatest vulnerabilities facing transit systems, a survey methodology was developed. Surveyors ask respondents to rate the vulnerability of a transit system to certain forms of terrorist attacks. They then compile the information and identify and rank those areas of greatest concern. In the initial demonstration of the survey conducted using in-house counterterrorism consultants, the survey showed:

Underground rail
Maintenance and fuel storage facilities
Control and communication centers
Receipt rooms

are particularly vulnerable to different types of terrorist threats. It further indicated that certain weapons available to terrorists will be favored in different types of attack. Explosives led the list followed by incendiary explosives, hand-held conventional and sophisticated weapons, and non-lethal chemicals. While the data presented is very limited being based on only two responses and was shown primarily to show how the survey data should be analyzed, it is recommended that additional interviews be conducted to obtain conclusive results.

The study concluded that there is a strong possibility that mass transit systems will become the target of some terrorist act. Their accessibility, the number of people who could be affected, and the amount of disruption that could be caused to parallel transportation modes if the population avoided mass transit make such an act very attractive to terrorists. The nation's transit systems have little or no ability to prevent a dedicated act of terrorism. The recommendations focus on the need to be able to respond to the threat of a terrorist act quickly, with trained and equipped personnel; to share intelligence information nationally allowing early identification of threats; and finally, to examine each system individually, assessing threat and vulnerability, and to allow those resources to become available for use where needed.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

The potential occurrence of hostage situations and indiscriminant acts of terrorism is of growing concern in the United States. In view of large number of persons carried by bus, train, or subway at any given time, the large urban mass transit systems offer tempting targets for terrorists. The principal reasons are that:

- Attacks receive wide publicity
- Disruptions to service have a large economic impact
- Large amounts of cash are handled by the system.

Attacks which can publicize and possibly remunerate terrorists are particularly attractive targets.

The combined efforts of federal, state, and municipal law enforcement agencies, along with individual transit security staffs, have focused on maintaining normal passenger security. However, even with the proper focus, these organizations cannot ensure that transit systems will be secure from terrorism or sabotage. An example of this is the success that partisan forces have had operating in a closed society under martial law. In our open society, protecting the transit system will be a very difficult project.

1.1 Purpose

This study was commissioned to investigate the current state of security within transit systems and to provide recommendations for improvement of transit security.

1.2 Background

The U.S. Department of Transportation (DOT), through both the Transportation Systems Center (TSC) and the Urban Mass Transportation Administration (UMTA), has addressed transit security in numerous publications. DOT, through the Transportation Safety Institute, even provides training programs on transit security. However, no comprehensive, coordinated effort addresses the wide range of problems facing transit properties trying to deal with transit security. For instance, intelligence

1

collection, analysis, and dissemination are the keys to monitoring suspicious activity and tracking the footprints that lead to a terrorist act. System designs and operational strategies need to be developed to lower transit vulnerability. Training programs for security and rescue personnel need further development. However, there is no single focus for addressing these requirements.

Over the years, development and employment of improved technology have increased the safety and security of passengers and transit systems as a whole. The transit systems within the United States have employed technology to address passenger security, revenue security, employee security, facility security, vandalism, and so forth. However, the terrorist is often unpredictable, unorthodox, and even suicidal. Terrorist methods run counter to our open technological society, where technology thrives on repetition, standardization, and manageable risk. Although the terrorist may have a wide range of technology arrayed against him, he can often slip through the defenses of a society dependent on technology simply by acting primitively. Good intelligence, coupled with in-place, tested, and proven anti-terrorism procedures, can enhance our ability to defend ourselves.

The Transportation Systems Center, the Urban Mass Transportation Administration, the Transportation Safety Institute, and several large urban properties such as Washington and New York have addressed the possibility of terrorism in the United States. Policy, plans, and procedures have been studied and recommended that could assist in thwarting or discouraging attacks; however, without a team approach that combines intelligence collection and dissemination, security procedure development, and effective employment of technology, no system for anti-terrorism will be effective.

1.3 Tasking

This project was conducted in two phases. The first phase involved a survey of current transit system security precautions and visits with the Port Authority Transit and Washington Metropolitan Area Transportation Authority (WMATA) security personnel. It also involved a review of literature and data bases that provide information on terrorist activities. The second phase involved the development and use of a threat and vulnerability assessment survey to provide guidance on the most beneficial areas of counterterrorism. This report summarizes the results of these efforts.

2

1.4 Overview of Study

This report addresses safety and security of mass transit systems in general and specifically the terrorist element that is posing a threat to these systems. Section 2 examines the current state of transit system security and cites terrorism as a special case. Section 2 also defines terrorism and cites the current resource limitations to counteract the terrorist.

Section 3 describes the threat and vulnerability survey developed to provide insight into the priority of problems facing the transit properties; it discusses initial results and makes suggestions as to where research resources can be best spent.

Sections 4 and 5 offer conclusions that can be drawn from study as well as corresponding recommendations for enhancing security to meet the terrorist threat.

2. PRESENT STATE OF TRANSPORTATION SECURITY

The present state of transportation security especially as it relates to possible terrorist attack, is poor. In even the basic safety and security programs, there can be questions since not all mass transit systems have detailed and adequate emergency action plans to cover fire, flooding, criminal acts, mechanical or electrical failures, accidents, and medical emergencies. Existing system plans and procedures need to be reviewed for accuracy and appropriateness of response in light of new threats. Transit systems also need to execute interagency agreements that address individual responsibilities in areas involving multiple jurisdictions. Simulations, studies, and analyses need to be conducted by various government agencies to test transit safety and security programs. Conclusions and recommendations drawn from such tests have been incorporated into transit systems' operational plans and emergency action procedures. However, with few exceptions such as the WMATA hostage-taking demonstration, transit systems do not normally address terrorism as safety or security concern. Rarely have practical demonstrations been conducted to demonstrate the use of state-of-the-art security measures and counter-measures against a broad spectrum of terrorist scenarios. So, while some activity has taken place, the benefits have not yet filtered down to the local transit systems. This leaves the systems very vulnerable to terrorist activity.

2.1 Security

Types of transit system security may be generally categorized as physical safety and criminal security. To date, most transit systems have not had to deal with the threat of terrorism.

2.1.1   Physical Safety

Safety planning consists of two phases: a preventive phase and a reactive phase. The preventive phase is concerned with preventing an incident or accident while the reactive phase is concerned with the incident or accident response and minimizing its effect. Guidelines[1] and programs developed over the years have helped properties achieve a reasonable degree of safety in their transit systems. These guidelines address emergency action plans, employee training facilities, and equipment (passenger stations,

---

[1] "Recommended Emergency Preparedness Guidelines for Transit Systems" DOT-TSC-UMTA-84-26, March 1985, reprint October 1985

trainways, central controls), and vehicles. The guidelines also address the exchange of information among transit systems.

2.1.2   Criminal Security

Mass transit systems have always experienced crime problems. However, professional expertise is available within transit systems and from other municipal resources to utilize modern technology to assist in countering the criminal threat. Analyses[2] and case studies[3] have been conducted that explore and define the criminal problems. The technology necessary to counter these problems involving passenger security, employee security, revenue security, security of transit property, and white collar crime has been developed and is available. Security problems are known, and in some properties, are being addressed through education and training, improved equipment, facilities design, better policing, and utilization of state-of-the-art technology. Other properties are not addressing the problem, but that is more of an economic decision than a capability decision.

2.1.3   Terrorist Security

Security against terrorism is a unique but growing and highly visible aspect of the overall transit security program. Of all the guidelines, standards, and procedures considered in this study none came to our attention that dealt explicitly with the threat posed by terrorism. The range of problems that a terrorist can create is probably far greater than can ever be completely defended against. However, because most properties have completely ignored this problem, transit systems are much more vulnerable than they need be. Certain actions must be taken to make current safety and security procedures more effective against the terrorist threat. These actions include adopting a standard definition of terrorism, developing laws that allow the rapid focusing of law enforcement assets on a terrorist incident, and developing specific technology and operational practices aimed at thwarting terrorism or reducing its impact.

---

[2] "Transit Security: A Description of Problems and Countermeasures," DOT-TSC-UMTA-84-22, October 1984, reprint May 1985

[3] "Case Studies of Transit Security on Bus Systems," UMTA-VA-06-0088-83-1, August 1983, reprint June 1984

2.2   Special Case of Terrorism

Although plentiful literature has evolved in the past decade to help satisfy the popular demand for means of coping with terrorism, it tends to be ideological and vague about the terrorist threat. As an academic discipline, the writing on terrorism tends to be non-specific concerning a strict definition of what separates terrorism from criminal activity.   During the course of this study, it was difficult to identify a universally accepted definition of transit terrorism. The following definitions used by the FBI seem to cover the important elements that constitute a terrorist act:

> "Terrorism: Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
>
> "Terrorist Incident: A terrorist incident is a violent act or an act dangerous to human life in violation of the criminal laws of the United States or of any state to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
>
> "Terrorist Incident Prevented: A documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity."

To counter terrorism and provide safe transit systems through development of effective anti-terrorism programs, mass transit systems need to agree on what they are addressing. The definitions listed above can form the basis for such an agreement.

2.2.1   Understanding the Definition

There are two types of terrorist: ethno-nationalists, such as the IRA or the PLO, who are held together by linguistic, religious, and territorial links; and idealogically motivated groups, such as the Red Brigades or the right-wing death squads in Latin America. Although their motives may differ from those of the common criminal, it is often difficult to perceive any differences in their activities. As a matter of fact, many of their activities (e.g., kidnapping for ransom, bank robbery, and extortion) are identical. However, terrorism has demonstrated indiscriminate violence aimed at mass intimidation and social disruption that renders conventional criminal defenses much less effective. Additionally, the tendency toward fanaticism and self-sacrifice for a cause introduces

new problems for a criminal security system which assumes that even a criminal will react in a manner consistent with self-preservation.

The only way to distinguish a terrorist act from a criminal act is through the perpetrator's motive. The above definition does just that since it rests on a determination whether the purpose of an act is to further a political or social objective. The entire activity can then be classified as a terrorist act, and a much wider range of law enforcement resources can be dedicated to counterterrorism.

The practical matter of determining motive is a more difficult question. For this, law enforcement officials must initially rely on information provided by the perpetrators themselves. They will have to announce, in one way or another, that their purpose is to further a political cause by means of warning calls, announcements during the activity, or claims for credit after the act. However a motive is made public, the determination that an activity is terrorist in nature is necessary in order to provide a proper response.

2.2.2   Limited Legislation

Excerpts from two federal statutes that directly affect interstate transit systems are provided below. Both were enacted pursuant to a prior crisis but are still germane to this issue. The Hobbs Act states:

> "It is a violation (of Federal Law) for anyone to obstruct, delay, or affect commerce by robbery, extortion or to attempt or conspire to do so or to threaten physical violence to persons or property in furtherance of a plan or preparations to do anything in violation of this section."[4]

The Interstate Commerce Act cites the following as violations:

> "It is a violation to transmit in interstate commerce, any message containing any demand or request for ransom for the release of any kidnapped person.

> "It is a violation for anyone, who with intent to extort from any person, firm, association, or corporation, money or anything of value which is transmitted in interstate commerce and threatens to kidnap any person or threatens to harm another."

> "It is a violation for anyone to threaten to kidnap or harm another through the use of interstate commerce."[5]

---

[4] The Hobbs Act, Title 18, Section 1951
[5] Interstate Commerce Act, Title 18, Section 875 (selected portions)

These statutes, along with the criminal codes of local, state, and territorial jurisdictions, address various terrorist threat methods that require gratification of a demand. However, none of the laws, emergency action plans, or interagency agreements adequately addresses the terrorist threat within the United States. Furthermore, there are no guidelines or standards in place to assist transit systems in addressing the terrorist threat.

2.2.3   Response Limitations

Numerous federal and state agencies can be utilized as resources in countering a terrorist act. Unfortunately, there are no formal lines of intelligence sharing to allow the rapid authorization of a response to terrorist threats. Isolated informal procedures for joint cooperation allow local law enforcement or transit agencies to work with and request assistance from the Federal Government, but in most cases, it takes as many as 36 to 48 hours to secure authorization of needed resources. Even then, questions of jurisdictional responsibility can arise. Such delays are inadequate when dealing with a rapidly developing terrorist threat.

There have been programs which have demonstrated effective structures for joining federal and local forces. The New York City Joint Task Force (JTF) is an example of what can be accomplished and could be used as a model for other large cities. The FBI first experimented with the JTF concept in 1979, when the bank robbery problem in New York City had grown to epidemic proportions. It became clear to the leadership of the New York City Police Department and the FBI that an innovative solution was required to address an increasingly dangerous situation. Accordingly, a formalized agreement, sealed by a signed memorandum of understanding, was entered into by the agencies. Detectives and FBI agents were detailed to a newly created task force jointly supervised by the FBI and New York City Police Department in order to eliminate duplication of effort, share resources, and foster cooperation.

The experiment is working. In a very real way, the Joint Task Force has become more than a sum of its parts. The skills and knowledge possessed by the police officers complement those of the agents, and a spirit of cooperation has replaced counter-productive competitiveness. The number of bank robberies has declined dramatically, and the solution rate has soared.

This precedent having been established, a Joint Terrorist Task Force was established in New York in 1980.

> "This Task Force, in its six years of existence has been successful in the investigation of numerous domestic and international terrorist groups operating in the United States. Its success was instrumental in the establishment of the much larger task force for the Los Angeles Olympics. It also has encouraged the planning of similar task forces in Chicago, New Haven, Newark, San Francisco, Los Angeles, Boston, and Washington, D.C. to address specific terrorism problems in those areas. "[6]

2.2.4 Terrorism as a Special Case

Terrorism is a special case of criminal activity because it has certain characteristics that distinguish it from other criminal activity. A definition of terrorism has to rely on the motivation of the terrorists rather than the terrorist act itself. A determination of intent is important since the proper response can only be initiated after the motive identified is concluded to be terrorist. The legislation against transit terrorism is very limited only affecting interstate systems such as New York and Washington. But, there have been successful efforts at joint local/federal law enforcement cooperation. Most notable is the Joint Terrorist Task Force established in New York in 1980. Terrorism must continue to be addressed as a special situation, and new emphasis must be placed on legislation concerning how terrorism will be handled.

2.3 Counterterrorism Assets

The U.S. currently uses a very layered approach in responding to terrorist activity. This layered response can include:

- Transit security forces
- Local police, fire, and rescue forces
- State police
- State National Guard

---

[6] Ambassador R. Oakley, Department of State speech, 16 June 1986

- Federal law enforcement personnel
  - Federal Bureau of Investigation
  - Bureau of Alcohol, Tobacco and Firearms
  - Federal Protective Service
- Federal government intelligence assets
  - Federal Bureau of Investigation
  - Defense Intelligence Agency
  - Central Intelligence Agency.

However, in reality, only a very small part of these assets would ever be employed to counter a terrorist act. Most transit properties have no way of bringing these assets to bear on a terrorist incident. Their most likely response would be to notify the local police. The police, in turn, would alert the state police, and so on. Similarly, there is no established procedure to alert properties of potential terrorist threats. Even something as simple as a weekly threat alert would provide some forewarning of possible problems. Work must be done to coordinate both the downward flow of information and the upward mobilization of responses to terrorist activity.

The problem of counterterrorism assets is further complicated by the lack of training in counterterrorist tactics presently available at the local and state levels. For the most part, transit security and local police do not have the opportunity to receive specialized training. As a result, the initial shock of a well-coordinated terrorist attack could have a much greater effect than it might have if trained personnel were available to be brought in immediately.

Finally, the equipment available to transit security personnel is completely inadequate to counter a terrorist threat. To pose as an effective constraint to terrorist activity, transit police must have rapid access to tools, equipment, and firearms commensurate with the task at hand. It is understood that the civilian population would not accept the presence of a heavily armed transit security policeman, but there are ways of making weapons available without actually carrying them around. Moreover, the weapons need not be lethal; rather, any of a number of debilitating agents could be used either by a fixed or portable system.

As presently configured and supported, the wide range of assets available for counterterrorist activity pose little deterrence to a committed terrorist. Work needs to

be; done to coordinate law enforcement and intelligence dissemination activities. Furthermore a new emphasis must be placed on providing training and equipment support for security forces.

3. TRANSIT SYSTEM THREATS AND VULNERABILITIES

The second phase of this study developed a methodology to identify and prioritize specific problems U.S. transit systems face when they attempt to protect themselves from terrorism. One can quickly be overwhelmed by the challenge of trying to protect against all possibilities. Of primary importance is to prioritize the broad range of threats and identify the more significant vulnerabilities so that efforts can be focused where they will do the most good. The question was how to identify these particular problem areas.

One method is to survey experts with long-term experience in the anti- and counter-terrorism arena to determine what they believe are significant vulnerabilities. Another method is to survey historical terrorist activities to see what has been done in the past. A problem with the latter is that terrorist acts tend to evolve over time. Knowledge of what has gone before will not necessarily guarantee successful prediction of future terrorist targets. The survey should be structured to be used repeatedly in refineing the definition of the particular vulnerabilities as more experts are polled. A portion of this project was devoted to developing and employing an expert survey.

3.1 Survey Design

The specific purpose of the survey was to identify and prioritize the wide range of threats and vulnerabilities facing U.S. transit systems. These include hostage taking, hijacking, kidnaping, robbery, personal assault, facility destruction, and service disruption. But, threats do not occur in isolation; they must be weighed in light of their particular targets. In the case of transit systems, targets include trains, buses, stations, and other facilities. Vulnerabilities can be defined as the combination of a threat with a target. For example, the vulnerability of a station to its own destruction will differ from its vulnerability to involvement in a hostage situation. Similiarly, a power generation station will have differing degrees of vulnerability to disruption of service and robbery attempts.

The agent employed to carry out the threat is another important factor in determining vulnerability. Agents are those implements employed by terrorists in carrying out their attack. Potential agents include hand-held weapons, sophisticated weapons, explosives, incendiary devices, lethal and non-lethal chemical agents, electronic

12

means of disruption, and surreptitious activities such as unauthorized entry to nonpublic areas. It is easily seen that some targets may be more vulnerable to one type of agent than another. More importantly, if one can identify the most likely agents, one knows where to focus preventive measures.

The initial survey focused on a particular threat involving a single target category and a single agent. The factor, (high, medium or low) associated with these three items was an assessment of an individual vulnerability. Figure 3-1 shows one segment of the matrix created when the survey was conducted. In all, 96 assessments of vulnerability were made for each of the six threat categories.

THREAT AND VULNERABILITY MATRIX

SITES	THREATS / AGENTS	HOSTAGE POSSIBLE HIJACK					CHEMICAL		UNAUTHOR	SUB-
		ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	NON-LETH	LETHAL	ENTRY	TOTAL
STATIONS, TERMINALS, & DEPOTS	SURFACE	1	2	1	3	1	1	1	0	10
	UNDERGROUND	1	2	1	3	1	3	1	0	12
	ELEVATED	1	2	2	3	1	1	1	0	11
BUSES	BETWEEN STATIONS	1	2	1	3	1	1	1	0	10
RAIL	SURFACE	2	2	1	3	1	2	1	0	12
	UNDERGROUND	2	2	3	3	1	1	1	1	14
	ELEVATED	1	2	1	3	1	1	1	0	10
OTHER FACILITIES	MAINT.&FUEL STORAGE	0	2	1	3	2	2	1	3	14
	CONTROL CTR	2	2	1	3	2	1	1	3	15
	RECEIPT RM	3	2	2	3	1	1	1	3	16
	COMM CENTR	3	2	1	3	2	1	1	3	16
	GENERATION STATION	2	2	2	3	1	1	1	3	15
SUBTOTALS	STATIONS	3	6	4	9	3	5	3	0	33
	BUS	1	2	1	3	1	1	1	0	10
	RAIL	5	6	5	9	3	4	3	1	36
	FACILITIES	10	10	7	15	8	6	5	15	76
TOTAL ALL		19	24	17	36	15	16	12	16	155

Figure 3-1

Sample of Threat and Vulnerability Matrix

Although careful analysis of each site's vulnerability to a given threat and agent was useful, it still did not indicate clearly the likelihood of an event's occurrence. A given site may be vulnerable to attack, but that does not necessarily mean such an attack is likely. During a final review of the matrix, experts on counterterrorism were asked to provide an assessment of probability that a terrorist threat would be carried out at a particular site. Again, this assessment was high, medium, or low and is represented by the circled letter in Figure 3-1. Since one probability factor was assigned to each site, 72 separate estimates are provided.

Completing one sheet provided a great deal of raw data covering threats, sites, agents, and attack probability. However, to be useful, the data must be broken down and analyzed to see what general trends, if any, can be derived and to identify specific areas where significant threats were combined with high probabilities.

3.2 Source of Data

The demonstration of the survey technique was conducted during an interview with Mr. Ralph Murphy, a consultant to Advanced Technology; and Mr. Richard Clement, Technical Director of Advanced Technology's Security Group.

Mr. Murphy has over 30 years' experience in intelligence analysis, research, development, and applications of security systems. He has lectured at municipal, national, and international forums and conducted training programs directed toward crime prevention, methods of combatting contemporary violence, unconventional warfare, and anti-terrorism. Mr. Murphy has developed security controls and directed security enhancement programs for airports, seaports, banks, hospitals, hotels, and various types of government facilities. His experience in dealing with counterterrorism, together with his experience in the layout of transportation facilities, made him an excellent subject for this demonstration.

Mr. Clement has over 20 years' experience in intelligence analysis, physical security, hostage extraction, and counterterrorism. He participated in development of anti-guerilla systems in Vietnam to protect shipping and harbor facilities. He recently served as the head of the Federal Protective Service responsible for the protection of all Federal buildings and is currently Chairman of the American Defense Preparedness Association's

Security and Intelligence Division. His long history of involvement in issues of physical protection made him an ideal choice for the survey.

Messrs. Murphy and Clement prepared separate responses to the various security threats faced by urban mass transit systems. They then combined their responses on a single matrix. The matrix, shown in Appendix A, was the direct result of their work.

3.3 Survey Constraints

Certain assumptions were necessary in order to compile the vulnerability matrix. These assumptions involved the relationships between the various factors which make up the vulnerability of a particular site to a specific terrorist act. The following paragraphs describe these assumptions and discuss their impact on the results.

As was stated earlier, the vulnerability of a particular site is not constant under all circumstances. Vulnerability will vary depending on the type of act being committed. For instance, a bus is more vulnerable to hijacking than to an attack aimed at service disruption. Similarly, a maintenance facility is more vulnerable to facility destruction than to kidnapping or hijacking. Both the site and the threat have to be considered in estimating vulnerability; but these are not the only variables. The vulnerability of a site to a terrorist act also depends on the agent or weapons used to carry out the act. One agent may be more effective in a given situation than another. Again, as an example, a bus is more vulnerable to hijacking using a hand-held weapons than using electronic measures. When Messrs. Murhy and Clement filled out the matrix, they considered three factors at once. For each combination of site, threat, and agent, they judged the vulnerability to be high, medium, low, or not applicable.

Using high, medium, and low raises the question "relative to what are these vulnerabilities judged?" For this analysis, the vulnerability of the most common agent, namely the hand-held weapon, was judged to be the medium in almost all instances; thus other agents were rated relative to the hand-held weapon. The only exceptions were in personal assault, where the vulnerability to a hand-held weapon was judged high, and, in certain facility destruction threats, where the vulnerability to a hand-held weapon was judged to be low. In all instances, the vulnerability to specific weapons was judged relative to the hand-held weapon.

Another area of concern was the possible biasing of the report due to the numbers of sites in a transit system. The large disparity in the number of buses compared to the number of maintenance facilities could place an undue emphasis on the buses solely because of their higher number. This would result in a very low emphasis being placed on relatively high-value sites such as control centers, stations, and other fixed facilities. To overcome such bias, the experts treated the sites as total populations rather than individuals. The matrix shows what they considered to be vulnerabilities in general and not that associated with individual units.

With these assumptions in place, all 576 entries were made in the matrix, and the task became to determine where the priorities for transit security need to be placed.

3.4   Study Results

Since the purpose of this study was to determine the greatest risks facing transit systems, specific results of the study and its implications will be discussed in the following paragraphs. The first area to be examined is vulnerability of specific sites to individual threats. The same threats will then be examined to see how they are most likely to be carried out. The result will be an ability to focus on the greatest vulnerabilities and to discuss what should be done to better protect these assets.

The key vulnerability matrix shown in Figure 3-2 illustrates the significant vulnerabilities at both the high and low end; that is, the circled numbers indicate high vulnerability, while boxed numbers indicate low vulnerability. Vulnerabilities represented by zeros exist, but they do not warrant particular attention.

Review of the matrix suggests several possible generalizations. There appear to be two major threats to transit systems. The first is facility destruction, and the second is service disruption. But, where one would most likely expect threats directed toward buses, trains, and stations, greater vulnerability is in the transit facilities area. Maintenance yards, control and communications centers, and receipt rooms are indicated as the most likely sites for attack. With the exception of disabling a train in a tunnel to disrupt service, all other significant vulnerabilities are in the facilities area.

16

SIGNIFICANT SITE VULNERABILITIES

SITES	THREATS	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT
STATIONS, TERMINALS, & DEPOTS	SURFACE	0	0	6.4	0	0	0
	UNDERGROUND	0	0	6.4	0	0	0
	ELEVATED	0	0	6.4	0	0	0
BUSES	BETWEEN STATIONS	0	6.4	0	0	0	0
RAIL	SURFACE	0	6.4	6.4	0	0	0
	UNDERGROUND	0	6.4	6.4	0	0	0
	ELEVATED	0	6.4	6.4	0	0	0
OTHER FACILITIES	MAINT. & FUEL STORAGE	0	0	6.4	0	(20.4)	(20.4)
	CONTROL CTR	0	0	6.4	0	(20.4)	(18)
	RECEIPT RM	0	(18)	(20.4)	5.6	0	0
	COMM CENTR	(16)	0	6.4	0	(19.2)	(18)
	GENERATION STATION	0	6.4	6.4	4.8	(15.6)	(15.6)

Figure 3-2

Significant System Vulnerabilities

17

Looking at the specific facilities, the same four sites share high vulnerability to differing threats. The maintenance yard and control center would be key targets in either a facility destruction or service disruption effort. The communications center shares this vulnerability and adds the possible development of an assault resulting in a hostage situation. This may be due to the greater access to media from a communications facility. Finally, the receipt room is particularly vulnerable in three areas: kidnapping or extortion, robbery, and physical destruction.

On the low side, kidnapping and robbery should not be looked on as posing a significant terrorist threat to transit systems. While both could occur, the chances are low that a terrorist would attempt either when more lucurative and lower exposure opportunities elsewhere. Similarly, generating stations, which include transformer buildings, are not often vulnerable to threats against person and are not likely targets for this type of attack.

Taken as a whole, the matrix indicates that attention needs to be focused toward the major transit facilities with an eye toward making them less susceptible to destruction and distributing system operation and control over a broad area with sufficient back-up equipment to ensure that no single attack could close the system. The area that was of concern was the vulnerability of the receipt room. However, despite current safeguards, a dedicated terrorist attack could easily defeat most systems, and the returns for such success would be significant. Other vulnerabilities that did not rate high in the matrix should be addressed, but only after the more significant ones are identified.

In Figure 3-3, which illustrates the agents being used for various threats, clear targets for research become apparent. The threat of facilities destruction and service disruption through use of explosives or incendiary devices are significant. Destruction using a sophisticated weapon and the use of a non-lethal chemical, such as tear gas, to disrupt operations are both significant threats. To a lesser extent, mainly because the vulnerability of the site to the threat is lower, the use of explosives in hijacking and personal assault and the use of hand-held weapons in personal assaults represent threats which stand out.

SIGNIFICANT AGENT THREATS

AGENTS THREATS	ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	CHEMICAL		UNAUTHOR ENTRY
						NON-LETH	LETHAL	
HOSTAGE/HYJACK	0.00	0.00	0.00	12.00	0.00	0.00	0.00	0.00
KIDNAP	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.20
ROBBERY	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60
PERSONAL ASSAULT	1.40	10.40	0.00	10.60	0.00	0.00	0.00	0.40
FACILITY DESTRUCTN	0.00	0.00	9.80	11.80	10.93	0.00	0.00	1.73
SERVICE DISRUPT	0.00	0.00	0.00	10.93	9.33	10.13	0.00	1.93

Figure 3-3
Significant Threat Agents

19

Examining the low threats shows that unauthorized entry is not a significant problem. Since the public has access to almost any place a terrorist might want to strike, the need for unauthorized entry is very low. The use of electronics for personal assault is obviously not a threat.

The zeros again illustrate threats which are not insignificant but which should be addressed after those of greater concern.

The survey described above has certain limitations which need to be addressed. Most significant is that it represents the opinions of only two individuals. Although they are recognized authorities, it is still only the opinion of two men. The process of filling out the matrix and then reducing and analyzing the data tries to rank the suspected vulnerabilities and threats. The use of standard deviation to arrive at a cutoff point was not absolutely necessary. Other methods could have been used, but standard deviation does provide a repeatable framework for additional data collection, verification and refinement of these initial results. We have provided a blank matrix disk so that additional surveys can be conducted and data collected. A clear picture of priorities will develop as this process continues. The priorities will most likely shift over time as the terrorist mentality changes, as improvements are made to transit system defenses, and as society adjusts to the threat. Continued use of this or similar surveys can provide an early alert to changes in terrorist operations and give the researcher an opportunity to quickly identify new threats.

4. CONCLUSIONS

As a result of this study, the following conclusions are offered for consideration:

- Traditional security and safety of mass transit systems seem to be adequate. There have been numerous studies and guidelines published dealing with conventional safety and criminal security. There are policies, procedures, and operating plans at most properties that cover facilities and equipment, personnel (employee/passenger), training, and emergency action procedures including inter-departmental relationships.

- When addressing terrorist security in transit systems, the picture changes. There are no guidelines or standards published that will assist the security professional in dealing with this threat. With a few exceptions, the properties have not taken any steps to protect themselves from the special threat of terrorism.

- The preparation of property, facilities, and personnel to counter a terrorist threat has been lacking at most properties. Similarly, the first line of defense against terrorism is not equipped to confront most terrorist assaults.

- Research areas can be identified and projects developed to allow an effective transit counterterrorism project to be designed and implemented.

- The current relationship between agencies (local through federal) except those cities undertaking the joint task force (JTF) concept can take as many as 36 to 48 hours to be invoked; this is unacceptable in a terrorist situation, and provision should be made to broaden the scope of the JTF concept or streamline interagency cooperation.

- Simulations and practical demonstrations have been conducted by transit properties to exercise in-place policies and procedures related to traditional security. Except for the WMATA demonstration, few practical demonstrations have been conducted against the terrorist scenario and applicable state-of-the-art security countermeasures.

21

5. RECOMMENDATIONS

The following is a list of recommendations resulting from this study:

- Conduct site surveys of selected mass transit systems and categorize the type of transit asset needed on the basis of socioeconomic, environmental, geographical, and political climates.

- Conduct the proposed survey using numerous transit system security and other law enforcement personnel to establish a baseline for proposing new counterterrorism research.

- Establish matrices to provide quantitative and qualitative priorities from which a transit system data base can list threats, vulnerabilities, and evaluation criteria.

- Establish an official or unofficial network that will share information obtained by both technological and nontechnological means through the Joint Task Force (JTF) concept.

- Recommend new legislation to make federal resources immediately available for JTF operation wherever mass transit is federally supported.

- Plan and conduct practical adversarial demonstrations against state-of-the-art security measures and terrorism countermeasures.

APPENDIX A

Threat and Vulnerability Survey Matrix

The enclosed survey technique was prepared to facilitate the compilation and analysis of UMTA security information. The technique consists of filling out two matrices, the Threat and Vulnerability Matrix and the Probability of Terrorist Activity Matrix, based on the answers of expert respondents. A series of supporting matrices are automatically completed and highlight the areas of significant terrorist risk.

LOTUS 1-2-3 version 1.0 was employed to prepare the spreadsheet. Figure A-1, on the following page provides a map of the TSC/UMTA Security spreadsheet showing the locations of all entries. The pages following Figure A-1 provide printouts of the individual matrices for UMTASEC1. WKS, the sample survey described in Section 3 of the report. Finally, the disk provided with this report contains both UMTASEC1.WKS and UMTASEC0.WKS, the latter is a blank copy of the spreadsheet which can be copied and used to conduct additional surveys.

Figure A-2 consists of matrix pages and provides the contents of the Threat and Vulnerability Matrix. Each page consists of a single type of threat, such as, hijack, robbery, etc. The matrix was filled out by the respondent who indicated a vulnerability of high, medium, low, or not applicable for each sub-element of the threat. Figure A-3 summarizes the Threat and Vulnerability Matrix by summing the values for each individual threat. Figure A-4 is the second matrix which must be filled out by the respondent. In it, the respondent indicates the relative probability of the different threats occuring over a range of urban transit targets. The next three matrices, Figure A-5, A-6 and A-7 displays the product of figures A-2 and A-3; the sum-of-squares standard deviation calculations, and the vulnerability values judged to be significant by the fact that they lie outside the range of standard deviation.

Similarly, Figures A-8, A-9 and A-10 provide the same summary, standard deviation and significant value displays but for the terrorist agents such as hand-held weapons, chemicals, explosives, etc., which might be employed by a terrorist.

To use UMTASEC0.WKS to perform additional surveys, copy the file and complete the Threat and Vulnerability Matrix and the Probability of Terrorist Activity Matrix. The others will be automatically filled in when the new inputs are calculated.

Should the original UMTASEC0.WKS spreadsheet be used, the Clear Probability and Clear Threat and Vulnerability Matrices can be used to restore the clear spreadsheets for future use. They are set up to replace only the data input records without disturbing the formula entries.

	A	N	Y	AJ	AU	BF	BQ BS
1	TITLES	THREAT AND VULNERABILITY MATRIX					TOTALS
		HOSTAGE	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DESTRUCTION	SERVICE DISRUPTION

UMTASEC0.WKS
LOTUS 123 VERSION 1.0

50 — T&V MATRIX SUMMARY

100 — PROBABIL- ITY OF TERRORIST ACTIVITY

150 — VULNERA- BILITY TIMES PROBA- BILITY | STD. DEV. CALCULA- TIONS | SIGNIFICANT VULNERABILITY VALUES

200 — CLEAR PROBABILITY MATRIX

	BU	CJ	CW
200	AGENT SUMMARY	STD. DEV. CALCULATIONS	SIGNIFICANT AGENT VALUES

250 — CLEAR T&V MATRIX
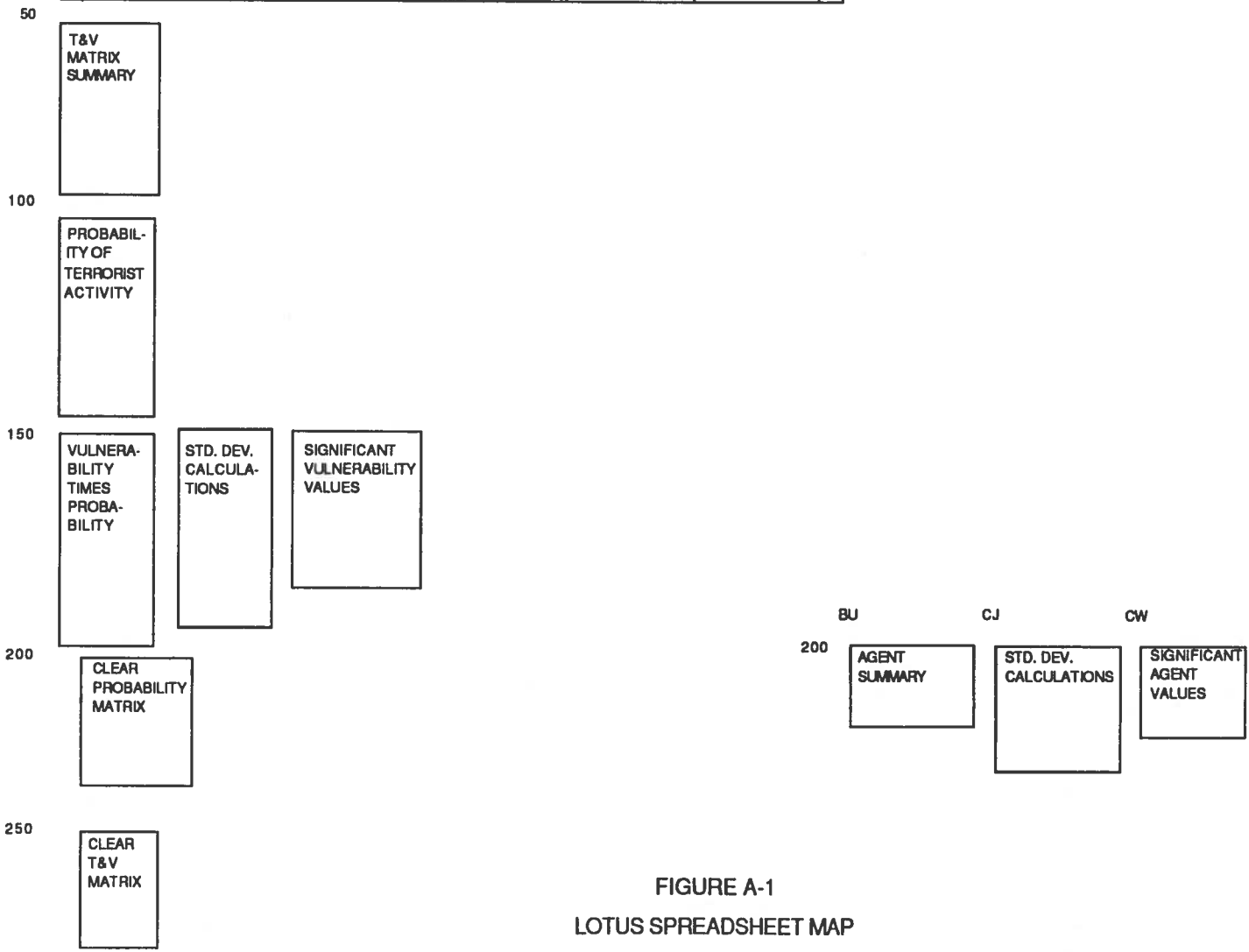
FIGURE A-1

LOTUS SPREADSHEET MAP

THREAT AND VULNERABILITY MATRIX

SITES	AGENTS	HOSTAGE POSSIBLE HIJACK					CHEMICAL		UNAUTHOR	SUB-
		ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	NON-LETH	LETHAL	ENTRY	TOTAL
STATIONS, TERMINALS, & DEPOTS	SURFACE	1	2	1	3	1	1	1	0	10
	UNDERGROUND	1	2	1	3	1	3	1	0	12
	ELEVATED	1	2	2	3	1	1	1	0	11
BUSES	BETWEEN STATIONS	1	2	1	3	1	1	1	0	10
RAIL	SURFACE	2	2	1	3	1	2	1	0	12
	UNDERGROUND	2	2	3	3	1	1	1	1	14
	ELEVATED	1	2	1	3	1	1	1	0	10
OTHER FACILITIES	MAINT.&FUEL STORAGE	0	2	1	3	2	2	1	3	14
	CONTROL CTR	2	2	1	3	2	1	1	3	15
	RECEIPT RM	3	2	2	3	1	1	1	3	16
	COMM CENTR	3	2	1	3	2	1	1	3	16
	GENERATION STATION	2	2	2	3	1	1	1	3	15
SUBTOTALS	STATIONS	3	6	4	9	3	5	3	0	33
	BUS	1	2	1	3	1	1	1	0	10
	RAIL	5	6	5	9	3	4	3	1	36
	FACILITIES	10	10	7	15	8	6	5	15	76
TOTAL ALL		19	24	17	36	15	16	12	16	155

FIGURE A-2

(1 of 6)

THREAT AND VULNERABILITY MATRIX

SITES	THREATS / AGENTS	KIDNAP ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	CHEMICAL NON-LETH	CHEMICAL LETHAL	UNAUTHOR ENTRY	SUB-TOTAL
STATIONS, TERMINALS, & DEPOTS	SURFACE	1	2	1	1	1	3	1	0	10
	UNDERGROUND	1	2	1	1	1	3	1	0	10
	ELEVATED	1	2	1	1	1	3	1	0	10
BUSES	BETWEEN STATIONS	1	2	1	1	1	1	1	0	8
RAIL	SURFACE	1	2	1	1	1	1	1	0	8
	UNDERGROUND	1	2	1	1	1	1	1	0	8
	ELEVATED	1	2	1	1	1	1	1	0	8
OTHER FACILITIES	MAINT.&FUEL STORAGE	1	2	1	1	1	1	1	2	10
	CONTROL CTR	1	2	1	1	1	1	1	3	11
	RECEIPT RM	3	2	1	1	1	3	1	3	15
	COMM CENTR	3	2	1	1	1	3	1	3	15
	GENERATION STATION	1	2	1	1	1	1	1	0	8
SUBTOTALS	STATIONS	3	6	3	3	3	9	3	0	30
	BUS	1	2	1	1	1	1	1	0	8
	RAIL	3	6	3	3	3	3	3	0	24
	FACILITIES	9	10	5	5	5	9	5	11	59
TOTAL ALL		16	24	12	12	12	22	12	11	121

FIGURE A-2

(2 of 6)

THREAT AND VULNERABILITY MATRIX

SITES	THREATS AGENTS	ROBBERY ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	NON-LETH	CHEMICAL LETHAL	UNAUTHOR ENTRY	SUB-TOTAL
STATIONS, TERMINALS, & DEPOTS	SURFACE	1	2	1	1	1	1	1	0 :	8
	UNDERGROUND	1	2	1	1	1	1	1	0 :	8
	ELEVATED	1	2	1	1	1	1	1	0 :	8
BUSES	BETWEEN STATIONS	1	2	1	1	1	1	1	0 :	8
RAIL	SURFACE	1	2	1	1	1	1	1	0 :	8
	UNDERGROUND	1	2	1	1	1	1	1	0 :	8
	ELEVATED	1	2	1	1	1	1	1	0 :	8
OTHER FACILITIES	MAINT.&FUEL STORAGE	1	2	1	1	1	1	1	0 :	8
	CONTROL CTR	1	2	1	1	1	1	1	0 :	8
	RECEIPT RM	3	2	2	2	1	3	1	3 :	17
	COMM CENTR	1	2	1	1	1	1	1	0 :	8
	GENERATION STATION	1	2	1	1	1	1	1	0 :	8
SUBTOTALS	STATIONS	3	6	3	3	3	3	3	0 :	24
	BUS	1	2	1	1	1	1	1	0 :	8
	RAIL	3	6	3	3	3	3	3	0 :	24
	FACILITIES	7	10	6	6	5	7	5	3 :	49
TOTAL ALL		14	24	13	13	12	14	12	3 :	105

FIGURE A-2

(3 of 6)

A-6

THREAT AND VULNERABILITY MATRIX

SITES	THREATS / AGENTS	PERSONAL ASSAULT					CHEMICAL		UNAUTHOR ENTRY	SUB-TOTAL
		ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	NON-LETH	LETHAL		
STATIONS, TERMINALS, & DEPOTS	SURFACE	1	2	2	3	3	1	3	0	15
	UNDERGROUND	1	2	2	3	3	1	3	0	15
	ELEVATED	1	2	2	3	1	1	3	0	13
BUSES	BETWEEN STATIONS	0	3	1	3	2	1	1	0	11
RAIL	SURFACE	0	3	3	3	2	1	1	0	13
	UNDERGROUND	0	3	3	3	3	1	3	0	16
	ELEVATED	0	3	3	3	1	1	1	0	12
OTHER FACILITIES	MAINT.&FUEL STORAGE	0	3	1	2	1	1	1	0	9
	CONTROL CTR	0	3	1	2	1	1	1	0	9
	RECEIPT RM	0	2	1	1	1	1	1	0	7
	COMM CENTR	2	3	1	2	1	1	1	2	13
	GENERATION STATION	0	1	1	1	1	1	1	0	6
SUBTOTALS	STATIONS	3	6	6	9	7	3	9	0	43
	BUS	0	3	1	3	2	1	1	0	11
	RAIL	0	9	9	9	6	3	5	0	41
	FACILITIES	2	12	5	8	5	5	5	2	44
TOTAL ALL		5	30	21	29	20	12	20	2	139

FIGURE A-2

(4 of 6)

THREAT AND VULNERABILITY MATRIX

SITES	THREATS AGENTS	I	FACILITIES DESTRUCTION					CHEMICAL NON-LETH	LETHAL	UNAUTHOR ENTRY	SUB-TOTAL	I
		I	ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND			:		I
STATIONS, TERMINALS, & DEPOTS	SURFACE	I	1	2	2	3	3	1	1	0 :	13	I
	UNDERGROUND	I	2	2	1	3	3	1	1	1 :	14	I
	ELEVATED	I	0	2	3	3	1	1	1	0 :	11	I
BUSES	BETWEEN STATIONS	I	0	1	3	3	3	1	1	0 :	12	I
RAIL	SURFACE	I	0	1	3	3	3	1	1	0 :	12	I
	UNDERGROUND	I	0	1	3	3	3	1	1	0 :	12	I
	ELEVATED	I	0	1	3	3	3	1	1	0 :	12	I
OTHER FACILITIES	MAINT.&FUEL STORAGE	I	2	2	3	3	3	2	1	1 :	17	I
	CONTROL CTR	I	3	2	1	3	3	2	1	2 :	17	I
	RECEIPT RM	I	3	2	1	2	3	1	3	2 :	17	I
	COMM CENTR	I	3	2	1	3	3	1	1	2 :	16	I
	GENERATION STATION	I	1	2	3	3	1	1	2	0 :	13	I
SUBTOTALS	STATIONS	I	3	6	6	9	7	3	3	1 :	38	I
	BUS	I	0	1	3	3	3	1	1	0 :	12	I
	RAIL	I	0	3	9	9	9	3	3	0 :	36	I
	FACILITIES	I	12	10	9	14	13	7	8	7 :	80	I
TOTAL ALL		I	15	20	27	35	32	14	15	8 :	166	I

FIGURE A-2

(5 of 6)

A-8

THREAT AND VULNERABILITY MATRIX

SITES	THREATS AGENTS	SERVICE DISRUPTION ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	CHEMICAL NON-LETH	LETHAL	UNAUTHOR ENTRY	SUB-TOTAL
STATIONS, TERMINALS, & DEPOTS	SURFACE	3	2	1	1	1	3	1	1	13
	UNDERGROUND	3	2	2	3	1	3	1	0	15
	ELEVATED	2	2	3	3	1	3	1	0	15
BUSES	BETWEEN STATIONS	1	2	1	3	3	3	1	0	14
RAIL	SURFACE	1	2	2	3	3	3	1	0	15
	UNDERGROUND	2	2	3	3	3	3	1	0	17
	ELEVATED	2	2	3	3	1	1	1	0	13
OTHER FACILITIES	MAINT.&FUEL STORAGE	2	2	1	3	3	2	1	3	17
	CONTROL CTR	2	2	1	3	3	2	1	1	15
	RECEIPT RM	3	2	1	1	3	1	1	3	15
	COMM CENTR	2	2	1	3	3	2	1	1	15
	GENERATION STATION	1	2	1	3	3	2	1	0	13
SUBTOTALS	STATIONS	8	6	6	7	3	9	3	1	43
	BUS	1	2	1	3	3	3	1	0	14
	RAIL	5	6	8	9	7	7	3	0	45
	FACILITIES	10	10	5	13	15	9	5	8	75
TOTAL ALL		24	24	20	32	28	28	12	9	177

FIGURE A-2

(6 of 6)

THREAT AND VULNERABILITY SUMMARY MATRIX

SITES	THREATS	I	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT
STATIONS, TERMINALS, & DEPOTS	SURFACE	I	10	10	8	15	13	13
	UNDERGROUND	I	12	10	8	15	14	15
	ELEVATED	I	11	10	8	13	11	15
BUSES	BETWEEN STATIONS	I	10	8	8	11	12	14
RAIL	SURFACE	I	12	8	8	13	12	15
	UNDERGROUND	I	14	8	8	16	12	17
	ELEVATED	I	10	8	8	12	12	13
OTHER FACILITIES	MAINT.&FUEL STORAGE	I	14	10	8	9	17	17
	CONTROL CTR	I	15	11	8	9	17	15
	RECEIPT RM	I	16	15	17	7	17	15
	COMM CENTR	I	16	15	8	13	16	15
	GENERATION STATION	I	15	8	8	6	13	13
SUBTOTALS	STATIONS	I	33	30	24	43	38	43
	BUS	I	10	8	8	11	12	14
	RAIL	I	36	24	24	41	36	45
	FACILITIES	I	76	59	49	44	80	75
TOTAL ALL		I	155	121	105	139	166	177

FIGURE A-3

PROBABILITY OF TERRORIST ACTIVITY MATRIX

SITES	THREATS	I	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT
STATIONS, TERMINALS, & DEPOTS	SURFACE	I	0.8	0.8	0.8	1.0	1.0	0.8
	UNDERGROUND	I	0.8	0.8	0.8	1.0	1.0	0.8
	ELEVATED	I	0.8	0.8	0.8	1.0	1.0	0.8
BUSES	BETWEEN STATIONS	I	1.0	0.8	1.0	1.0	0.8	0.8
RAIL	SURFACE	I	0.8	0.8	0.8	0.8	1.0	0.8
	UNDERGROUND	I	0.8	0.8	0.8	0.8	1.0	0.8
	ELEVATED	I	0.8	0.8	0.8	0.8	1.0	0.8
OTHER FACILITIES	MAINT.&FUEL STORAGE	I	0.8	0.8	0.8	0.8	1.2	1.2
	CONTROL CTR	I	1.0	1.0	0.8	1.2	1.2	1.2
	RECEIPT RM	I	0.8	1.2	1.2	0.8	0.8	0.8
	COMM CENTR	I	1.0	1.0	0.8	1.0	1.2	1.2
	GENERATION STATION	I	0.8	0.8	0.8	0.8	1.2	1.2
SUBTOTALS	STATIONS	I	2.4	2.4	2.4	3.0	3.0	2.4
	BUS	I	1.0	0.8	1.0	1.0	0.8	0.8
	RAIL	I	2.4	2.4	2.4	2.4	3.0	2.4
	FACILITIES	I	4.4	4.8	4.4	4.6	5.6	5.6
TOTAL ALL		I	10.2	10.4	10.2	11.0	12.4	11.2
NORMALIZED SUBTOTALS	STATIONS	I	0.8	0.8	0.8	1.0	1.0	0.8
	BUS	I	1.0	0.8	1.0	1.0	0.8	0.8
	RAIL	I	0.8	0.8	0.8	0.8	1.0	0.8
	FACILITIES	I	0.9	1.0	0.9	0.9	1.1	1.1
TOTAL ALL NORMALIZED		I	3.5	3.4	3.5	3.7	3.9	3.5

FIGURE A-4

VULNERABILITY TIMES PROBABILITY SUMMARY MATRIX

SITES	THREATS	I	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT
STATIONS, TERMINALS, & DEPOTS	SURFACE	I	8.0	8.0	6.4	15.0	13.0	10.4
	UNDERGROUND	I	9.6	8.0	6.4	15.0	14.0	12.0
	ELEVATED	I	8.8	8.0	6.4	13.0	11.0	12.0
BUSES	BETWEEN STATIONS	I	10.0	6.4	8.0	11.0	9.6	11.2
RAIL	SURFACE	I	9.6	6.4	6.4	10.4	12.0	12.0
	UNDERGROUND	I	11.2	6.4	6.4	12.8	12.0	13.6
	ELEVATED	I	8.0	6.4	6.4	9.6	12.0	10.4
OTHER FACILITIES	MAINT.&FUEL STORAGE	I	11.2	8.0	6.4	7.2	20.4	20.4
	CONTROL CTR	I	15.0	11.0	6.4	10.8	20.4	18.0
	RECEIPT RM	I	12.8	18.0	20.4	5.6	13.6	12.0
	COMM CENTR	I	16.0	15.0	6.4	13.0	19.2	18.0
	GENERATION STATION	I	12.0	6.4	6.4	4.8	15.6	15.6
SUBTOTALS	STATIONS	I	26.4	24.0	19.2	43.0	38.0	34.4
	BUS	I	10.0	6.4	8.0	11.0	9.6	11.2
	RAIL	I	28.8	19.2	19.2	32.8	36.0	36.0
	FACILITIES	I	67.0	58.4	46.0	41.4	89.2	84.0
TOTAL ALL		I	132.2	108.0	92.4	128.2	172.8	165.6
NORMALIZED SUBTOTALS	STATIONS	I	8.8	8.0	6.4	14.3	12.7	11.5
	BUS	I	10.0	6.4	8.0	11.0	9.6	11.2
	RAIL	I	9.6	6.4	6.4	10.9	12.0	12.0
	FACILITIES	I	13.4	11.7	9.2	8.3	17.8	16.8
TOTAL ALL NORMALIZED		I	41.8	32.5	30.0	44.5	52.1	51.5

FIGURE A-5

SITE STANDARD DEVIATION

SITES	THREATS	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT	SITE TOTALS
STATIONS, TERMINALS, & DEPOTS	SURFACE	9.610	9.610	22.090	15.210	3.610	0.490	60.6
	UNDERGROUND	2.250	9.610	22.090	15.210	8.410	0.810	58.4
	ELEVATED	5.290	9.610	22.090	3.610	0.010	0.810	41.4
BUSES	BETWEEN STATIONS	1.210	22.090	9.610	0.010	2.250	0.010	35.2
RAIL	SURFACE	2.250	22.090	22.090	0.490	0.810	0.810	48.5
	UNDERGROUND	0.010	22.090	22.090	2.890	0.810	6.250	54.1
	ELEVATED	9.610	22.090	22.090	2.250	0.810	0.490	57.3
OTHER FACILITIES	MAINT.&FUEL STORAGE	0.010	9.610	22.090	15.210	86.490	86.490	219.9
	CONTROL CTR	15.210	0.010	22.090	0.090	86.490	47.610	171.5
	RECEIPT RM	2.890	47.610	86.490	30.250	6.250	0.810	174.3
	COMM CENTR	24.010	15.210	22.090	3.610	65.610	47.610	178.1
	GENERATION STATION	0.810	22.090	22.090	39.690	20.250	20.250	125.2

SUM OF SQUARES............. 1224.64

VARIANCE.................. 17.25

STANDARD DEVIATION......... 4.15

MEAN..................... 11.10

MEAN MINUS STD. DEV........ 6.95

MEAN PLUS STD. DEV......... 15.25

FIGURE A-6

SIGNIFICANT SITE VULNERABILITIES

SITES	THREATS	HOSTAGE POSSIBLE HIJACK	KIDNAP	ROBBERY	PERSONAL ASSAULT	FACILITY DISTRUCTN	SERVICE DISRUPT
STATIONS, TERMINALS, & DEPOTS	SURFACE	0	0	6.4	0	0	0
	UNDERGROUND	0	0	6.4	0	0	0
	ELEVATED	0	0	6.4	0	0	0
BUSES	BETWEEN STATIONS	0	6.4	0	0	0	0
RAIL	SURFACE	0	6.4	6.4	0	0	0
	UNDERGROUND	0	6.4	6.4	0	0	0
	ELEVATED	0	6.4	6.4	0	0	0
OTHER FACILITIES	MAINT.&FUEL STORAGE	0	0	6.4	0	20.4	20.4
	CONTROL CTR	0	0	6.4	0	20.4	18
	RECEIPT RM	0	18	20.4	5.6	0	0
	COMM CENTR	16	0	6.4	0	19.2	18
	GENERATION STATION	0	6.4	6.4	4.8	15.6	15.6

FIGURE A-7

A-14

NORMALIZED AGENT SUMMARY

THREATS	ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	CHEMICAL NON-LETH	LETHAL	UNAUTHOR ENTRY	TOTAL
HOSTAGE/HYJACK	5.7	8.0	5.4	12.0	4.6	5.2	4.0	3.3	48.2
KIDNAP	4.8	8.0	4.0	4.0	4.0	6.8	4.0	2.2	37.8
ROBBERY	4.4	8.0	4.2	4.2	4.0	4.4	4.0	0.6	33.8
PERSONAL ASSAULT	1.4	10.4	7.0	10.6	7.3	4.0	6.7	0.4	47.8
FACILITY DESTRUCTN	3.4	6.0	9.8	11.8	10.9	4.4	4.6	1.7	52.7
SERVICE DISRUPT	7.3	8.0	6.7	10.9	9.3	10.1	4.0	1.9	58.3
TOTAL	27.0	48.4	37.1	53.5	40.2	34.9	27.3	10.2	278.6

The top-left header cell reads "AGENTS" (above) and "THREATS" (below).

FIGURE A-8

AGENT STANDARD DEVIATION

THREATS	ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	CHEMICAL NON-LETH	LETHAL	UNAUTHOR ENTRY :	SUB-TOTAL
HOSTAGE/HYJACK	0.019	4.822	0.163	38.388	1.450	0.365	3.255	6.105 :	54.6
KIDNAP	1.008	4.822	3.255	3.255	3.255	0.992	3.255	12.990 :	32.8
ROBBERY	1.972	4.822	2.573	2.573	3.255	1.972	3.255	27.083 :	47.5
PERSONAL ASSAULT	19.397	21.122	1.430	23.000	2.338	3.255	0.744	29.205 :	100.5
FACILITY DESTRUCTN	5.780	0.038	15.967	35.950	26.308	1.972	1.450	16.572 :	104.0
SERVICE DISRUPT	2.338	4.822	0.744	26.308	12.455	18.742	3.255	14.983 :	83.6
TOTAL	30.5	40.4	24.1	129.5	49.1	27.3	15.2	106.9 :	423.1

SUM OF SQUARES.............. 423.079

VARIENCE................... 9.002

STANDARD DEVIATION......... 3.000

MEAN...................... 5.804

MEAN MINUS STD. DEV........ 2.804

MEAN PLUS STD. DEV......... 8.804

FIGURE A-9

SIGNIFICANT AGENT THREATS

THREATS	ECCM	HAND WEP	SOPH WEP	EXPLOSIVE	INCIND	NON-LETH	CHEMICAL LETHAL	UNAUTHOR ENTRY
HOSTAGE/HYJACK	0.00	0.00	0.00	12.00	0.00	0.00	0.00	0.00
KIDNAP	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.20
ROBBERY	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60
PERSONAL ASSAULT	1.40	10.40	0.00	10.60	0.00	0.00	0.00	0.40
FACILITY DESTRUCTN	0.00	0.00	9.80	11.80	10.93	0.00	0.00	1.73
SERVICE DISRUPT	0.00	0.00	0.00	10.93	9.33	10.13	0.00	1.93

FIGURE A-10