Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs

Peter deLeon, Brian Jenkins, Konrad Kellen, Joseph Krafcheck

A Report prepared for SANDIA LABORATORIES
The research described in this report was sponsored by Sandia Laboratories under Contract No. 05-4946.

Reports of The Rand Corporation do not necessarily reflect the opinions or policies of the sponsors of Rand research.
Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs

Peter deLeon, Brian Jenkins, Konrad Kellen, Joseph Krofcheck

A Report prepared for SANDIA LABORATORIES
This report identifies and describes the possible attributes of potential criminal adversaries of U.S. nuclear programs, and the characteristics of potential adversary actions, particularly those that might result in serious consequences for public health and safety. It represents a portion of a continuing research project sponsored by Sandia Laboratories, and satisfies the report requirements described in Task 2 of the Threat Analysis Study.

The analysis is based on case materials compiled on various categories of criminal and terrorist activities that might be analogous to future threats against U.S. nuclear facilities. Companion research on the intentions of possible nuclear adversaries is in progress. This report should be of particular interest to agencies whose responsibilities include the security of facilities that house nuclear programs and the safeguarding of nuclear materials.
SUMMARY

This report describes the attributes of groups or individuals who might carry out criminal actions against nuclear programs in the United States. In this context, the term "attributes" refers to the physical resources, planning skills, and methods of operation that the potential adversary might assemble and use. "Actions" refers to criminal actions against nuclear installations or to the theft of nuclear materials. We have assembled this information to help designers of security systems develop appropriate criteria for protecting nuclear facilities against armed attacks or sabotage, to guard nuclear materials against theft and diversion, or to deal effectively with any such episodes should they occur.

The principal methodological problem in conducting such research is that there have not been a great number of serious actions directed against U.S. nuclear facilities that can be examined. To the best of our knowledge, no nuclear installations in the United States have been attacked, seized, or sabotaged in a way that caused the release of radioactive materials. No nuclear weapons have been stolen or illegally detonated. No nuclear materials have been diverted or taken by force from installations or while in transit and used for blackmail or made into bombs. And no radioactive matter has been maliciously released so that public safety was endangered. Therefore, we have collected and examined several hundred incidents of criminal, terrorist, or paramilitary actions that are in some way analogous to nuclear incidents. The explicit assumption is that the analogs can provide knowledge and insights into the capabilities and modus operandi of various types of potential adversaries of nuclear programs.

ANALOG CATEGORIES

It is realized that important differences in adversary intentions, capabilities, and actions may exist between crimes for personal gain or politically motivated terrorist activities and possible attacks on nuclear installations or the theft of special nuclear materials or
weapons. Still, certain attributes and actions observed in the analog categories would be required of any adversary engaged in nuclear mischief. For example, both criminals and nuclear adversaries gather intelligence, force entry, and assemble assault teams. By studying analog activities, we can gain a great deal of information pertinent to the design of nuclear facility defense systems. For this study, we selected the following analog categories for examination: (1) task force crimes, i.e., major armed robberies and burglaries; (2) terrorist assaults; (3) military commando raids; (4) industrial sabotage; and (5) symbolic bombings. In addition, we examine and describe a limited number of domestic and foreign nuclear incidents in which there was a serious threat to public safety.

Task force crimes were examined because they represent criminal assaults on well-protected targets or facilities (such as bank vaults, arsenals, and museums), often demonstrating remarkable planning, technical skills, and execution. In the 45 cases reviewed, criminals were able to assemble teams of as many as twenty people (yet remain undiscovered), breach thick walls and vaults and neutralize modern alarm systems, and devote up to 2 years of planning for a single "caper." Task force members often displayed considerable technical competence (e.g., in overcoming electronic alarm systems) but little inclination to accept a high risk of capture or death.

Thirty-four terrorist assaults were reviewed because, in general, they involved individuals who were highly dedicated and willing to accept great personal risks. Unlike the professional criminals, terrorists were quick to brandish weapons and explosives. Still, they rarely assaulted facilities when the probability that they might be defeated before they gained their objectives was very great. Terrorists almost always had highly political objectives as a primary purpose for their actions. For this reason, they chose very conspicuous targets that would certainly bring them publicity.

Seventy-five small-scale military and paramilitary commando raids were studied because they offered the only incidents in which well-armed, specially trained, and dedicated personnel attacked designated targets, usually with the explicit intent of destroying them. Also,
commando operations provided the only instances of assaults against well-defended targets. They are particularly relevant because they highlight the importance of accurate intelligence and the element of surprise. These two attributes were central in explaining the extraordinary high success rate (close to 80 percent) of the commando raids, which is particularly remarkable because the attacks were against defended targets.

Industrial sabotage against private industry, transportation facilities, and public utilities is an obvious analog. Our examination showed that the saboteur's objective was the destruction or disruption of facilities or equipment on a significant scale. Industrial sabotage is especially relevant to possible nuclear sabotage because saboteurs typically have privileged information or access. The 40 incidents that we surveyed revealed that the saboteurs had a wide range of motivations (including something as simple as being a disgruntled employee or a rejected suitor) and usually chose unprotected targets. Generally speaking, saboteurs were strongly risk averse and did not deliberately endanger the lives of the general public. Their disproportionately high effectiveness (in terms of accomplishing their objectives), achieved by a limited number of people with minimal means (in one case, literally one person with a few bolts) and at low personal risk, was largely due to an accurate knowledge of the facility's operations and vulnerabilities, as well as access to restricted areas.

Over one hundred cases of symbolic bombings are part of our analog data base. A "symbolic bombing" is defined as a deliberate act of violence calculated to express a grievance or to make a political statement; the damage to, or destruction of, the target may be secondary, or even irrelevant to the adversary's aims. We included symbolic bombings in our data base because nuclear facilities are viewed by some as symbols of unwarranted and dangerous technology and might therefore be subjected to such bombings. Our survey showed that bombs were usually placed on unprotected targets. The bombers did not display a great deal of technical expertise or dedication; indeed, they were almost cavalier in their approach to their activities.

Finally, a number of nuclear incidents were examined, even though
they are not, of course, analogs. Between 1969 and 1975, there were 288 known recorded threats against, or incidents at, nuclear facilities in the United States. Almost all of these (240) were only bomb threats, but there were 9 actual bombings, 22 cases of arson or suspected arson, and a variety of miscellaneous actions (e.g., felling a meteorological tower or pranks). A serious fire was set at the Indian Point nuclear power reactor. One widely publicized case in which nuclear materials were removed from the controlled area occurred at a fuel fabrication plant in Oklahoma, and that involved only a very small amount. Thus, even though the overall number of nuclear incidents within the United States is quite high, the number of serious threats to the public safety has been very low.

Overseas, however, there has been a larger number of serious nuclear incidents. Perhaps more important, they have been increasing in frequency and possible danger. For example, in France between 1975 and 1976, there were 8 major explosions at French nuclear facilities (such as reactors, processing plants, and uranium mines). In England, 20 uranium fuel elements were stolen from the Bradwell nuclear power station in 1966; the elements were recovered when the culprits tried to sell them. In March 1973, a leftist urban guerrilla group temporarily occupied an atomic power plant under construction at Atucha, Argentina; the reactor had not been installed.

"Typical" Analog Activities

Using an analytic framework designed jointly by Rand and Sandia personnel, the analog incidents were coded and examined for common features, including adversaries' aims and objectives, their personnel and equipment resources, their means of transportation, access and egress, and the amount of time required to carry out a given action. From these codings, "typical" analog activities were extracted.

A "typical" burglary was one done by two to four professional criminals who were technically skilled and intent on avoiding any confrontation with security forces; they were usually armed but refrained from using their weapons. The members of the team were carefully chosen, both for their technical skills and degree to which they could
be trusted. A "typical" armed robbery team had three to six members who were somewhat less skilled than their burglar counterparts; they were more willing to use weapons, but usually as a means of discouraging possible resistance; again, they were highly risk averse. A "typical" terrorist assault team consisted of three to six men armed with automatic weapons, grenades, and explosives; they were highly dedicated to a given political cause; they were well trained but not particularly sophisticated in technical skills. A "typical" military commando raid often engaged large numbers of men (in one case, over 200), but many were carried out with as few as three or four men. The commandos were well armed and well trained (as befits a military operation), had explosives, and carried whatever equipment was necessary to accomplish their mission. They were technically skilled in the use of their equipment. The "typical" industrial sabotage incident was accomplished by either a single individual or a group of six or more people. Saboteurs were rarely well armed, but their access to special information and restricted areas permitted them to identify the critical vulnerabilities of their targets and cause a great deal of damage. Like the burglar and armed robber, saboteurs had little incentive for confronting security systems or gaining personal publicity. A "typical" symbolic bombing was politically motivated and was carried out by one or two people (although there is evidence that they often had the support of a larger organization) who were not particularly skilled in a technical sense. The bombs were generally simple. Some of the bombers were characterized by strong but volatile loyalty and dedication, floating in and out of a number of sympathetic groups. The main purpose of their activities was political recognition; hence, a political, written communique usually accompanied their bombs.

COMPOSITE ADVERSARIES

From these "typical" analog incidents and the range of attributes around the modal values, two composite adversaries were constructed: a "typical composite profile" and a "high-level composite." The "typical composite profile" was derived from all the analogs, with the exception of the commando raids. It represents a level of resources
and skills that criminal and political adversaries have commonly been able to assemble and, as such, might be able to assemble were an adversary group to target a nuclear facility. It consists of three to six adversaries, armed with automatic weapons, possessing high explosives and hand and power tools, using a variety of ground transportation modes, having middle- to high-level technical skills and a varying willingness to accept high risks, possessing some inside information or assistance, and displaying a moderate to high degree of ingenuity and careful advanced planning. The typical composite profile represents one reference point on a scale of adversary capabilities.

The "high-level composite" aggregates the high-level attributes thus far observed in real-life episodes, although not necessarily the highest levels. It provides another reference point on a scale of adversary capabilities, obviously much higher on the scale than the typical composite profile. If the typical composite profile summarizes those attributes that are commonly seen, the high-level composite represents something near the upper bounds. The commando raids were not included in the high-level composite because they took place in a wartime environment, and we are concerned here with adversaries who plausibly might appear in a peacetime environment. It should be noted, however, that in most of the attributes the high-level composite resembles the typical commando raid, except that commandos are unlikely to have inside assistance, an attribute that we ascribe the high-level composite here.

The high-level composite consists of twelve to twenty perpetrators who have a wide range of weapons, including light crew-served weapons, possess high explosives and power tools, and have inside information and assistance, high levels of criminal and military skills, and dedication, ingenuity, and imagination. The high-level composite also has a wide range of modern communications equipment, at least adequate financing, experience in its specialties, and the ability to maintain secrecy and achieve tactical surprise.

It should be emphasized that the appearance of the high-level composite, with all the high-level attributes, is an unlikely event; the simultaneous appearance of all the characteristics has not appeared
in any single adversary in the data base, with the possible exception of a few wartime commando raids. There are several reasons why this is so. First, it is difficult to assemble such a combination of skills and personnel. Second, such a combination might not have been perceived as necessary. Third, some of these high-level attributes are mutually contradictory. For instance, the technical sophistication required to neutralize an electronic alarm system would be less important if the adversary planned to storm a facility with a large number of heavily armed men; similarly, the willingness to risk capture or death stands in partial contradiction to technical expertise, at least as seen in the present data base. This is equally true of the typical composite profile. The fact that such an assemblage has not been observed in any single adversarial group in the past does not imply that such a group could not be assembled in the future, especially given the large payoffs that nuclear facilities or programs might appear to offer to terrorist or criminal elements in terms of personal gain, political statements, or other possible incentives; but it should be reemphasized that nothing approaching the high-level composite has been observed in the peacetime data base.

The high-level composite helps us to identify which capabilities seem the hardest for an adversary to attain, and at what levels he begins to encounter difficulties. We refer to these levels as breaking points. Real-life adversaries have already demonstrated their ability to attain a high level in some attributes; in others they face greater difficulties.

**DESIGN OF DEFENSIVE SYSTEMS**

The composites suggest a number of implications for the design of a security system for nuclear installations. First, it does not appear that adversaries would have any particular difficulty in obtaining the physical resources needed to assault an installation. The number of men or the availability of weapons, explosives, and special equipment does not seem to be a critical restraint. Moreover, the evidence suggests that a small group of skilled people can be very effective. The adversary's critical constraints do not appear to lie
in the areas of physical resources. Rather, the pivotal attributes
determining the success of a venture appear to be the less tangible
human factors: imagination and ingenuity; criminal skills; technical
knowledge; the willingness to risk capture or death; accurate intel-
ligence and privileged access; the ability to achieve tactical surprise;
and the necessary combination of several of these.

It follows, then, that defensive systems might be designed to
exploit the critical human factors, i.e., to raise them to or above
the adversary's breaking point. It is difficult to collect a group
of people who are technically knowledgeable; who are skilled in such
things as the operation of weapons, the use of explosives, the circum-
vention of alarm systems, and the penetration of physical barriers;
and who are dedicated to the point of risking their lives but at the
same time will maintain the necessary group secrecy. A security sys-
tem that compels a potential adversary to possess all of these critical
human capabilities might deter or thwart a large number of the actions
that could be directed against it and the programs it is protecting.
It would, in effect, "price most potential adversaries out of the
market."

How might such a system be devised? First, it should be realized
that physical barriers are sufficient for delaying or hindering the
determined adversary but, by themselves, they cannot be expected to
defeat him. They require special attention or monitoring if they are
to prevent or hinder the adversary from gaining entry. Second, the
present data base suggests that the prospect of physical danger does
have some deterrent value, certainly to professional criminals and
even to some terrorists. Therefore, potential adversaries should be
aware that attempts to penetrate sensitive areas of nuclear facilities
will require them to risk their lives. Third, the deliberate creation
of uncertainty by the security system would appear to present the
greatest obstacles to potential adversaries in planning and executing
their acts. For example, an armed and trained guard force whose im-
mediate strengths and routines could never be confidently predicted
would make it extremely difficult for an adversary to know what levels
of attributes he would require, thus forcing him to assemble and employ
effectively all the capabilities and resources of the high-level composite. These measures would, in total, push the adversary toward his "breaking point," thereby making his task increasingly impossible.

A last implication for security systems emerged from the study of terrorist assaults that were characterized by high levels of personal dedication. Terrorists rarely assaulted facilities when there was a high probability that they might be defeated before they gained entry, but they were willing to assume high risks after they had gained entry and barricaded themselves. This finding implies that containment or reinforcement strategies would be less useful against terrorists whose mission, in their eyes, might be accomplished merely by gaining temporary control of a facility. Therefore, to deter nuclear terrorist assaults, the appropriate defenses must be structured to defeat any attack that might occur before the terrorists gain entry, rather than by trying to contain the assault after it is discovered.

Finally, this analysis is based on the current political, economic, and social conditions prevailing in the United States. There is little domestic unrest, violent activities have not been directed against U.S. nuclear facilities, and there is no evidence that professional criminals or terrorists are attracted to nuclear materials. Still, in the recent history of nuclear incidents, a subtle escalatory trend may be discerned, especially in light of the growing number of serious nuclear incidents in Europe in the past two years. Hence, it is important to recognize that the threat is largely a function of the political and social contexts upon which this analysis is based and that these contexts are subject to change. One cannot confidently predict that nuclear facilities will become a criminal or terrorist target in the future. But at the same time, one cannot ignore the dynamic nature of a threat that requires continual monitoring and reassessment as the relevant contexts change over time.
ACKNOWLEDGMENTS

This report is based on a series of case studies of criminal activities and political violence. The authors wish to acknowledge the contribution of those who researched and reported on these studies. Without the participation of Janera Johnson, Margaret Krahenbuhl, Geraldine Petty, Ralph E. Strauch, Eleanor S. Wainstein, and Martin L. Willinski, the report could not have been written. The authors would also like to acknowledge the intellectual contributions of two additional Rand colleagues, David F. Ronfeldt and Eliahu Zeira. The authors also owe a debt of gratitude to Carl Builder and Arturo Gandara, whose critical reviews greatly sharpened the focus of their thinking.

Personnel at Sandia Laboratories and the Department of Energy have been most helpful in their general support, guidance, and specific comments.
CONTENTS

PREFACE ................................................................. iii
SUMMARY .............................................................. v
ACKNOWLEDGMENTS .................................................... xv

Sections

I. INTRODUCTION ......................................................... 1
   Scope of the Research ............................................. 1
   Actions and Aims of Potential Adversaries .................. 2
   Organization of the Report ..................................... 5

II. METHODOLOGY ........................................................ 6
   Use of Analogs ..................................................... 7
   The Data Base ..................................................... 8
   Limitations to the Methodology ................................. 10

III. DISCUSSION OF DATA BASE ........................................ 11
   Task Force Crimes ................................................ 11
   Terrorist Assaults ............................................... 15
   Commando Raids .................................................. 18
   Industrial Sabotage ............................................. 21
   Symbolic Bombings .............................................. 23
   Nuclear Incidents ............................................... 25

IV. ANALYSIS OF THE DATA BASE ..................................... 32
   Classification and Coding ....................................... 32
   Aims and Objectives ............................................. 33
   Number of Adversaries ......................................... 33
   Armament and Equipment ....................................... 34
   Access and Egress ............................................... 35
   Duration ........................................................... 37
   Profiles ............................................................ 38
   "Typical" Analog Profiles ...................................... 39
   Typical Composite Profile .................................... 43
   The High-Level Composite Profile ............................ 46
   Implications of the High-Level Composite Profile ....... 50

V. CONCLUDING OBSERVATIONS ........................................ 54
   Critical Attributes .............................................. 54
   Possible Implications for Security Systems ................. 57
   Dynamic Nature of the Threat .................................. 60

Appendixes
A. THREAT CHARACTERISTICS OUTLINE ............................ 63
B. GLOSSARY .......................................................... 68
C. ADVERSARY ATTRIBUTES .......................................... 72
I. INTRODUCTION

This report describes the attributes of groups or individuals who might carry out criminal actions against nuclear programs in the United States. The purpose of the study is to assist officials responsible for formulating and designing security measures to protect U.S. nuclear programs by providing an understanding of the attributes of potential adversaries. In this context, we define "attributes" as referring to the physical resources, planning skills, and methods of operation that the potential adversary could assemble and use for some type of action against a nuclear facility or the theft of nuclear materials. This information can be used in the selection, development, and application of security techniques to protect nuclear materials from theft and diversion and to prevent the sabotage of nuclear facilities. It may also be useful for overall emergency contingency planning and even for possible negotiations with adversaries who might have successfully removed nuclear material or seized temporary control of a facility.

SCOPE OF THE RESEARCH

A principal research concern in describing possible adversary attributes and adversary action characteristics as they relate to potential attacks against nuclear installations has been to avoid speculation and scenarios as to how threatening the adversaries might be or what they might do. Incidents involving nuclear facilities or materials that have occurred to date do not provide an adequate basis for extrapolation to possible future actions against nuclear targets. This has led us to the detailed examination of other kinds of incidents that share some important characteristics with potential nuclear actions. We have examined criminal actions, politically motivated acts of violence, and paramilitary operations that have been carried out in the real world, events that contain elements analogous to potential actions directed against nuclear facilities or illicitly obtaining nuclear materials. These analogs include major armed robberies,
sophisticated burglaries, terrorist assaults and bombings, industrial sabotage, and commando raids. We have also examined incidents involving nuclear facilities or materials in the United States and abroad.

**ACTIONS AND AIMS OF POTENTIAL ADVERSARIES**

It is realized that there may be important differences in adversary motivation, attributes, and actions between crimes for gain or terrorist activity, such as bombings or assaults, and possible attacks on nuclear installations or the theft of special nuclear materials (SNM) or weapons. Still, adversaries who aim at nuclear mischief of any kind—be it theft, sabotage, malicious release, or destruction—must engage in actions and use methods also found in regular criminal acts: they must obtain extensive prior knowledge of objectives, installations, and routines; they must accomplish unauthorized entry by stealth, force, or deceit; they must successfully cope with alarm systems and armed guards; they may have to assemble teams; and they may have to recruit outside help. (The use of analogs and their link to nuclear incidents are discussed more specifically in Section II, "Methodology."

The threat to U.S. nuclear programs may be viewed as a spectrum of potential actions with consequences having varying degrees of severity. At the low end of this spectrum are acts such as bomb threats, hoaxes, and token acts of violence. None are aimed at producing serious public casualties or damage, but, if publicized, they could disrupt essential routines, alarm the populace, and discredit nuclear programs and safeguard measures. However, they would pose little direct danger to public safety. We recognize that the alarm created by a publicized nuclear threat or any malevolent action involving any nuclear facility, regardless of the reality of the threat or the degree of direct danger to the general population, could produce the spontaneous evacuation of surrounding off-site areas, panic, and casualties.

Higher on the scale of adversarial actions are those that could result in serious damage to a nuclear facility and endanger on-site personnel, although the acts or their consequences would not necessarily pose a serious threat to the safety of the general public.
Finally, there are actions directed against nuclear facilities that, if successful, could result in clear and serious danger to the public. Whereas actions at the lower end of the spectrum may be more probable and have potentially harmful consequences in terms of cost, alarm, and adverse publicity, it is the last category that most concerns us in this report, i.e., those actions whose ultimate consequences could be off-site civilian casualties, significant off-site material damage, and radioactive contamination. The most serious actions would result in the loss of nuclear weapons or special nuclear material and/or a radioactive release. Examples of this level of malevolent actions include stolen weapons or SNM that could be ransomed back to the original owners for cash or political concessions or sold to some third party on a black market. Stolen SNM also could be used in the construction (or alleged construction) of a nuclear explosive or perhaps dispersed as a toxin. The motivation to extract political concessions or obtain cash could lead to the seizure of a nuclear facility and threats to cause serious damage and radioactive dispersal if the demands were not met.

Neither of these actions—theft for sale or ransom or seizure of a facility—poses by itself a direct danger to public safety as long as it goes no further. However, once control over a weapon, SNM, or a nuclear facility has been lost, the potential risk of damage and of concomitant public alarm is so great that we must put these actions in the dangerous threat category. These last two actions clearly would imperil public safety.

Various aims of potential adversaries could lead to acts that could endanger public safety. Such aims could include attacks on government institutions with the purpose of eroding public confidence and exposing the government as unable to protect its citizens; a campaign to undermine public confidence in nuclear power; or simple publicity for an organization, cause, or belief. The adversaries could include political extremists (whose views might be clinically rational and internally consistent although quite different from those of society at large), lunatics, or criminals motivated by the desire for economic gain.
Adversaries' aims could be served either by the theft of nuclear weapons and SNM or by serious damage to a nuclear facility. Each of these tactical objectives could, in turn, be achieved by several means. SNM could be removed by the theft of marginal amounts of nuclear materials over a period of time until a dangerous amount were obtained. An attempt to steal weapons or SNM could be made by an insider acting alone, by burglars (possibly with inside collusion), or by means of armed robbery (overt attack). Serious damage to facilities might be caused by standoff attacks with mortars, bazookas, rocket-propelled grenades, precision-guided munitions, remotely piloted vehicles, or aerial bombardment. Damage could be inflicted by an insider or by persons who had gained illegal entry (as in a burglary), or it might be caused by saboteurs who had seized control of the facility itself.

The important point is that there is no single mode of attack but rather a variety of modes by which these tactical objectives could be achieved. Each mode has its own characteristics and each demands different capabilities on the part of the adversary. Each poses different problems for security.

We focus our primary attention in this report on those actions in which the adversaries are usually persons who are not employed in nuclear facilities or who do not have legitimate access to them and therefore must penetrate the facilities or sites to accomplish their mission. Hence pilferage and theft by insiders are not within the scope of this analysis because they involve exclusively or principally the actions of employees using techniques not covered by our current data base. In some ways, if physical damage to a facility is an objective, the standoff attack mode, which would not require penetration or even close approach by the perpetrators, appears to be the most attractive mode of attack because the risks for the attacker are less than in a frontal assault. It is not certain, however, what the effect of this type of attack would be on the targeted facilities. It would depend on the type of weapon used and on the physical features of the facility. These assessments are not within the scope of the present study. Therefore, the standoff mode of attack is not considered here except to identify it as a possible mode of action that merits further examination.
ORGANIZATION OF THE REPORT

The discussion and analysis that follow are divided into four sections. Section II contains a detailed description of the methodology of the research, particularly the problem of relating the non-nuclear analogs to potential nuclear actions. Section III reviews each of the six categories of analogs. Section IV offers a general overview and analysis of the data base. In it, we extract a number of adversary profiles and discuss how each might be relevant to the issue of nuclear facility safeguards. Section V contains the conclusions drawn from the preceding analysis. These pertain to the capabilities and resources of the potential adversaries, and to the security measures that might deter or defeat an attack or limit possible damage.
II. METHODOLOGY

Certain assumptions about the potential adversaries, their resources, and their methods of operation are prerequisites to the design of effective security systems. These assumptions may be arbitrary—i.e., intentions and capabilities may be arbitrarily assigned to the adversary—or the assumptions may be based on actual data. For example, there are thousands of bank robberies in the United States every year, a sufficient number to allow statistical inferences regarding their frequency, the number of perpetrators normally involved, the weapons and procedures used, the average "take," and other important variables.

It is necessary to make an assessment of the possible intentions and capabilities of potential adversaries of U.S. nuclear programs in order to develop appropriate measures to protect nuclear facilities against armed attack or sabotage, to guard nuclear materials against theft and diversion, or to prepare to deal effectively with any such episodes should they occur. The principal problem in conducting such research is that, unlike the case with bank robberies, a sufficient data base of actions directed against U.S. nuclear facilities does not exist. To the best of our knowledge, no nuclear installation in the United States has been attacked, seized, or sabotaged in a way that radioactive materials were released; no nuclear weapons have been diverted or illegally detonated; no nuclear materials have been stolen or taken by force from installations or in transit and used for blackmail or made into bombs; and no radioactive matter has been maliciously released so that public safety was endangered.

A number of bomb threats have been telephoned to nuclear facilities, a now common occurrence in both government and industry. A number of threats to use nuclear material have proved on investigation to be hoaxes. Minor sabotage has been carried out in a handful of cases. In one incident, a minute quantity of SNM was removed from a reprocessing facility. Although a certain amount of nuclear materials is unaccounted for, there is no available evidence that it was stolen or diverted in weapons use. Outside of the United States there have
been a few incidents of more serious potential consequences. Political extremists on two occasions attempted to sabotage nuclear reactors in France, and urban guerrillas temporarily seized control of a nuclear facility under construction in Argentina. These incidents are included in our discussion.

USE OF ANALOGS

In the absence of past major actions directed against nuclear programs, we have selected several categories of conventional crimes and political violence that can be regarded as coming closest in their aims and operations to possible but as yet uncommitted crimes against nuclear facilities or involving nuclear material. The explicit assumption is that a study of these analogs can provide knowledge and insights into the capabilities and the modus operandi of various types of potential adversaries of nuclear programs. Through the study of analogs, evidence may be acquired about methods by which objectives (such as theft, sabotage, or extortion) involving nuclear programs might be achieved.

An extremely important reservation to the use of the analog methodology when extrapolating the results of such a study to possible actions by adversaries against nuclear programs is that the analogous actions selected do not involve nuclear targets. However, sufficient similarities exist between the two types of action to allow certain inferences to be made regarding the attributes of possible nuclear adversaries. For example, while we know of no attempt in the United States to steal a shipment of plutonium or other special nuclear material, there is a richly documented history of well-planned burglaries and armed robberies of other valuable and protected commodities—e.g., cash, jewels, art objects. In many such cases, thieves were able to penetrate multiple and elaborate security systems to gain access and remove the materials. Similarly, an attack on a nuclear installation or the theft of nuclear materials must be conducted either by stealth or deceit, as in a burglary, or by force, as in a robbery. In material terms, the attack would require the adversaries to possess such resources as tools, weapons, transportation, and alarm suppressants;
in nonmaterial terms, it would require these same adversaries to dem-
onstrate such characteristics and attributes as daring, dedication, leadership, knowledge, or experience. The analogs offer examples of the means or assets that could be employed for such actions.

To give another example: Although there have been no publicized seizures or attempts to seize nuclear facilities except for the single incident in Argentina (and there the reactor was still under construc-
tion), there have been numerous forcible takeovers of buildings and seizures of hostages by terrorists. While political extremists in the United States have thus far not waged any campaigns of violence against nuclear facilities, they have claimed credit for bombings of government buildings, corporate offices, and public utilities. An examination of all of these actions offers possible insights into the style, dedication, and capabilities of groups that may select a nuclear target at some future date.

THE DATA BASE

Data have been assembled on several hundred incidents of different categories of analogs applicable in some specified ways to potential actions against nuclear programs. The primary criterion for selecting analog categories, or incidents within the categories, was that their attributes were closely analogous—in some instances identical—to what one might reasonably expect from a possible action against a nu-
clear facility. For this reason, the common street crimes and simple robberies were excluded from the data base. Even though such criminal actions might share some common features with an attack on a nuclear installation or repository, it was decided that the differences were too great to provide useful insights. A system that could defeat the more serious actions we examined would frustrate the lesser actions as well. This data base also helps to link motives or objectives with probable modes of action, and with the attributes of the most likely adversaries in each case. A list of the nonnuclear analogs that are being examined in this study, and their relationships to potential nu-
clear incidents, is shown in Table 1.
Table 1

ANALOGS BEING EXAMINED IN THE RAND STUDY

<table>
<thead>
<tr>
<th>Nonnuclear Analogs</th>
<th>Potential &quot;Nuclear Action&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbolic bombings and incidents of violence against symbolic targets.</td>
<td>Attempts by political or environmental extremists to carry out acts of symbolic violence against nuclear facilities.</td>
</tr>
<tr>
<td>Incidents of industrial sabotage and sabotage of vital systems (electric transformers, transmission lines, natural gas lines, etc.).</td>
<td>Sabotage of nuclear facilities.</td>
</tr>
<tr>
<td>Task force burglaries, robberies, and attempts to &quot;spring&quot; prisoners from the outside.</td>
<td>Well-planned penetrations of protected nuclear facilities for the purpose of theft or sabotage; hijacking of nuclear material in transit.</td>
</tr>
<tr>
<td>Paramilitary commando raids.</td>
<td>Well-planned, heavily armed assaults against defended nuclear targets (unlikely in current political environment).</td>
</tr>
<tr>
<td>Terrorist assaults on embassies, government buildings, small settlements, etc.</td>
<td>Armed assaults on nuclear facilities for the purpose of theft, sabotage, or seizing control of nuclear facilities.</td>
</tr>
</tbody>
</table>

An examination of the analogs provides insights into the capabilities that could be mobilized by an adversary in an action against nuclear facilities. It cannot provide assessments of the probabilities of occurrence of any action against nuclear programs, such as sabotage, theft of nuclear materials, symbolic bombings, or terrorist seizures.

It should not be inferred from our emphasis on a data base of analog events that it is possible to use rigorous quantitative methodology to predict or describe the threat. We are not dealing with a large enough data base to allow accurate statistical profiles. The sample is neither complete nor randomly chosen. The scope of the research project limited the coverage of analogous events. In many of the incidents examined, complete information was not available.
Furthermore, we do not have a full accounting of the cases that were deterred, let alone those that failed. We have not attempted to assign numerical probabilities or confidence intervals in the same way that other studies have estimated values of the occurrence of various types of accidents involving nuclear facilities. However, the events chosen are considered to be representative of their categories and adequate for eventually offering judgments about the "comparative likelihood"--as opposed to probability of occurrence--of certain kinds of action.

LIMITATIONS TO THE METHODOLOGY

There are limitations to this methodology. The data base is composed for the most part of incidents not involving nuclear targets. Nuclear targets might attract qualitatively and quantitatively different adversaries. Professional criminals and less dedicated terrorists might be dissuaded from mounting an operation against nuclear targets because nuclear commodities--unlike precious jewels and other normally stolen goods--have no ready street market or because of their expectation that nuclear facilities and material are likely to be better guarded. On the more pessimistic side, nuclear targets could attract adversaries with entirely different motivations and goals, e.g., the disruption or suspension of nuclear programs themselves. Potential adversaries might include those supported by foreign governments or by large well-financed political organizations with more resources than are likely to be possessed by a small band of professional criminals or political extremists. The anticipated gains from the successful theft of nuclear material might be considered so great as to warrant an effort hitherto unseen in the annals of conventional crime. In addition, their motivations could induce nuclear adversaries to assume greater risks than the analog perpetrators discussed in this study. Still, we can cautiously extrapolate the adversaries' capabilities and methods of attack from areas we regard as analogous on the basis of the similarities noted above.
III. DISCUSSION OF DATA BASE

At present, the data base contains descriptions of over 300 incidents of sophisticated or task force crimes (popularly called "capers") that had robbery or burglary as an objective, terrorist assaults, paramilitary commando raids, industrial sabotage, and symbolic bombings. In addition, known incidents involving nuclear facilities or materials in the United States and abroad were examined as part of the data base. However, because they are, in fact, nuclear incidents, not analogs, they are treated separately.

TASK FORCE CRIMES

The data base in this category is comprised of 45 crimes committed by groups of people, some of whom were highly specialized and skilled. These crimes were chosen because they were generally directed against closely guarded high-value targets and because they were especially well publicized, a feature that facilitated the data-collection effort. The perpetrators assembled for the specific operation and formed "task forces" organized for assaults on well-protected objectives, such as bank vaults, arsenals, prisons, and museums. The prizes sought were substantial, and some adversaries displayed sophisticated technical capabilities. The specialists involved in these crimes included safecrackers, electronic experts, and communications experts. About three-quarters of the task force crimes were committed in the United States and about one-quarter abroad, mostly in Great Britain and Canada. Most of the crimes were burglaries; the remainder were armed robberies, such as the famous Brinks' robbery in Boston, or attempts to "spring" prisoners from prison. Economic gains were the predominant motive. Except for one prison break and an arsenal robbery, both of which involved members of political extremist groups, none of the task force crimes had political overtones.

Almost all the incidents examined here were successful, in the sense that adversaries evaded or overcame the security measures and escaped with the "loot," at least for a certain time. It would be
instructive to examine failures as well, but information on them is difficult to obtain. Failures are generally not as well publicized as spectacular successes, which makes it difficult even to know about them. Unless the perpetrators are apprehended, we have few means of determining what resources they had assembled for their attempt. Moreover, professional criminals appear unwilling to assume major risks. Therefore, our means for determining when security measures deterred criminal acts are scarce, because no crimes were in fact committed. For these reasons, the capers sample must per force deal with crimes that were for the most part successful in terms of entry and escape, although not necessarily in avoiding ultimate arrest.

An examination of the capers shows that alarm systems do not always discourage or frustrate the more ingenious burglars, who may have a considerable capability for overcoming such systems. In one case, burglars drilled a hole in the exterior alarm box and injected into it a mixture of Freon and polyurethane, which formed a hard plastic foam and jammed the clapper on the bell. In another case, a vault's elaborate security system, including 12 television scanners, was penetrated without setting off an alarm. In a third case, thieves cut several 3-inch-thick cables that housed hundreds of wires leading to a communications center for several thousand burglar alarms, thus disarming the alarm systems for an entire area.

Burglars and robbers have often employed commercially available communications equipment, both for keeping in touch with each other during the operation and for monitoring police radio frequencies. During one bank robbery in 1954, the perpetrators isolated the bank by cutting the telephone cables while maintaining contact with the outside lookout via a walkie-talkie. Burglars in another caper monitored policeband radio broadcasts during and between stages of their operation.

The criminals studied here demonstrated the capability and patience required to engage in very long periods of reconnaissance and demanding preparations. Two different capers required 2 years of planning. Three wayward burglars spent 2 months tunneling 136 feet toward a bank's main vault, missing their mark by only 2-1/2 feet.
In most cases, particularly the burglaries, there was no evidence that the criminals were armed; weapons were not needed. However, in those instances in which weapons were considered necessary, the gang members were able to procure a variety of handguns, rifles, shotguns, machine guns, even a 20mm cannon. When the weapons were used, as in armed robbery, the criminals displayed overwhelming firepower, clearly with the intent to discourage resistance. Similarly, they were able to obtain both military and commercial types of explosives when they were needed.

Great attention was seemingly paid to avoiding violence during the execution of most burglaries and armed robberies. In the majority of cases, no violence was used, except that guns were held on the victims. In certain cases, limited violence (e.g., pistol whipping) was used to establish credibility and arouse fear, or possibly to speed up a recalcitrant guard.

Generally speaking, the criminals showed little inclination to risk capture or death. They usually selected lightly guarded targets, choosing to avoid rather than overpower guards. When the situation appeared dangerous, they would back off rather than accept the higher risk. Significantly, in two cases in which the motive was political rather than financial gain (an unsuccessful effort to spring inmates from prison and a successful raid on an armory in Canada), the adversaries seemed more willing to expose themselves to violence and to accept the attendant risk. (As we will see in the discussion of terrorist assaults where the motives are primarily political, the adversary was willing to assume a higher degree of risk and generally came prepared to fight if necessary.)

In several of the capers, inside help played an important role. In a $4.3 million robbery of an armored express company in 1974, the alleged participation of a security guard made forced entry unnecessary. In a burglary of the Bank of New Mexico branch at the Sandia facility in 1955, the police suspected that the culprits had an accomplice on the base. In a major airport robbery, the robbers may have had inside information, because, according to the police, they "went right to the shelf where the money was." In a 1975 art museum theft, the five
watchmen unwittingly (or perhaps otherwise) assisted the thieves by turning off the electronic burglar alarm system, "probably to be able to sleep," the museum's director stated.

Impersonation appears to be a ploy often used by robbers and burglars. Very importantly, in all cases studied where impersonation was used, it was successful. At an airport robbery in 1974, four armed men in hard hats, posing as telephone workers, gained entrance to a cargo building, handcuffed ten airline employees, and escaped with more than $200,000 in cash. In the Boston Brinks' robbery, the robbers' costumes resembled the uniforms of the Brinks' drivers. In the robbery of a U.S. mail truck in 1972, one of the robbers, dressed as a policeman, successfully flagged down the mail truck.

The number of perpetrators in any of the capers rarely exceeded seven, probably because more were not needed to carry out the act. A second possibility was that problems of recruitment and organization mitigated against larger numbers, as did considerations of dividing the loot and maintaining secrecy. The number of group members seemed to be geared to the various requirements of the crime, with at least one person in the group having a requisite specialty, such as wireman or communications expert. In some cases, tasks were "subcontracted" to nonparticipants (e.g., a locksmith charged with making keys). In most cases, the leader of the caper recruited members of the task force according to particular skills, often drawing upon a reservoir of former fellow convicts he had met in prison. In one instance, the group postponed the execution of their plan until a convict possessing a needed skill was released from prison. In another, participants were recruited from among members of a family.

The perpetrators displayed considerable talent for improvisation. One group used a 20mm cannon to penetrate a vault wall in a cellar by firing more than 30 rounds point-blank while protecting itself against shrapnel with a mattress. In another episode, when a lock from an outside door had to be removed for over an hour so that a duplicate key could be made, the perpetrators, faced with the possibility of arousing suspicion, made and attached a facsimile doorknob while the actual knob was at the locksmith's.
Criminals have created diversions to cause confusion and thus delay police reaction. For example, in one case armed robbers set off explosives in three locations and then carried out their robbery elsewhere.

On the whole, the perpetrators were seldom reckless in their actions. Recklessness is not the same as the willingness to engage in violence; the latter can be used without recklessness, if plans are well laid and well executed.

In sum, capers are analogs to, and offer possible insights for, a potential nuclear theft for a number of reasons. Both may require careful planning, execution, and specialized skills. The reluctance of sophisticated criminals to battle armed guards results in a reliance on deception, a modus operandi that might be used against nuclear facilities. Similar insights might be drawn from the criminals' demonstrated ability to neutralize modern detection and alarm systems.

**TERRORIST ASSAULTS**

This portion of the analog data base includes 34 terrorist assaults, which represents most of the terrorist assaults committed between 1968 and 1974.* Of these, 24 were related to the Arab-Israeli Middle East confrontation. The targets of many of these incidents were Israeli assets and citizens, including El Al offices and aircraft, diplomatic posts, and personnel outside Israel. Arab assets (e.g., embassies) were the targets of 2 incidents. American assets and citizens were involved in 6 incidents, including the Amman hotel seizure in 1970, the Lod airport attack in 1972, the seizure of the Bank of America in Beirut, and attacks on two parked aircraft in 1973. Three terrorist assaults took place in Latin America and 6 occurred elsewhere: the seizures of a train and the Indonesian Consulate in Amsterdam, the French Embassy in The Hague, the U.S. Embassy in Kuala Lumpur, and the West German Embassy in Stockholm; and an attack on a

---

San Francisco police station. The number of terrorists ranged from a single Arab terrorist in Athens to over 30 in Amman. Sixty-five percent of the incidents involved two to five actual attackers.

Terrorist assaults are particularly relevant to this study because they include many of the characteristics an adversarial force might employ in an attack against a nuclear facility. Terrorists can generally be seen as highly motivated and willing to assume great risks, two attributes we regard as potentially threatening in some types of possible action against nuclear facilities. Terrorists have been willing to attack in the face of certain armed and often lethal response; the Palestinian raid against Ma'alot is a pertinent example. In many cases, they permitted themselves to be surrounded, using hostages as their primary protection, even when security forces had repeatedly demonstrated a willingness to attack terrorists barricaded with hostages.

Three general features of the terrorists' assaults are particularly relevant to possible assaults against nuclear facilities. First, the terrorists involved were highly dedicated to their objectives and less deterred by the possibility of capture, injury, or death. Some terrorists—especially those operating in the Middle East situation—could be viewed as practically suicidal (e.g., the attack on Lod airport). Again, this willingness to expose themselves to extreme risk should not be confused with recklessness. Missions were usually carefully planned and executed. The terrorists rarely assaulted facilities when there was a high probability that they might be defeated before they attained their objectives. The point at which terrorists were willing to assume high risks was after they had attained their objectives (such as gaining entry and barricading themselves with hostages).

Second, the terrorists showed a strong proclivity to attack very conspicuous and politically significant targets, such as foreign embassies, where they could be assured of maximum visibility, press coverage, and public impact. Their actions enabled them to publicize their existence, cause, and demands to the widest possible audiences
and presented an opportunity to exercise leverage of a magnitude generally beyond the capability of relatively small groups. Five terrorists, claiming to be members of the Japanese Red Army, were able to gain significant concessions by holding hostages in the U.S. consulate in Kuala Lumpur for almost 80 hours. In some recent cases, terrorists holding hostages have barricaded themselves for several weeks.

Third, the terrorists' aims were almost always political. Every terrorist assault in the data base was characterized by demands for publicity, quite often by the publication of political manifestos; in only four (out of thirty-four) cases did the adversary groups attempt to extract money. These political aims call for a different set of security criteria from those assaults whose primary concerns are sabotage or theft. For instance, when the perpetrators of terrorist assaults wished to make their organizations and causes well known, they used threats against life and property, both to gain their demands and to effect their escape.

Several additional points regarding terrorist assaults can be briefly made. The attacking group, whatever its size, was almost always a part of a larger organization with resources the attackers could draw upon. The terrorists generally showed themselves capable of acquiring whatever arms and munitions were needed for their purposes, including automatic weapons, rocket-propelled grenades, and mortars. Similarly, they have been able to recruit sufficient manpower to meet their tactical requirements. Terrorist assaults generally have not demonstrated a particularly high degree of technical sophistication or training, but these skills were not usually required by their missions or aims. Seizing lightly guarded embassies and unprotected schoolrooms are not demanding tasks. Finally, they moved with great speed, often overcoming security measures before the alarm could be spread and defenses deployed. In the attack on the OPEC ministers' meeting in Vienna, a small band of terrorists was able to attack the building, seize their intended hostages, and seal off the area within 5 minutes.

In summary, terrorist assaults have been carried out by groups of highly dedicated people with primarily political aims against highly
visible targets. Often their choice of targets and threatened actions were designed to arouse strong emotions, thereby placing extraordinary pressures on political decisionmakers to accede to their demands; the actions of the South Moluccan terrorists in late 1975 and again in 1977 provide vivid testimony of this strategy. In every case, they achieved their publicity objective and they often gained their political objectives.

COMMANDO RAIDS

Seventy-five small-scale military and paramilitary commando and commando-type raids against a variety of targets and facilities were examined as analogs to assaults on nuclear facilities. These attacks covered the period from 1937 to 1977 and included raids by the Spanish loyalists, British and German commando groups during the Second World War, the Palmach and later Israeli raids, and Viet Cong and American commando raids during the Vietnam conflict. The number of participants ranged from two commandos who attacked parked aircraft during World War II to a group of over two hundred U.S. Rangers who stormed a Japanese-held island in the Pacific; the number of raiders averaged about twenty-seven.

Commando raids were added to the data base for two reasons. First, they offer examples of incidents in which well-armed, specially trained, dedicated personnel attacked designated targets, usually with the explicit intent of destroying them. Regardless of the likelihood, there is some possibility that a U.S. nuclear installation might be subjected at a future date to such an attack mounted by a well-financed and well-led terrorist organization. Second, military commando operations provide the only instances of assaults against well-defended targets. In most of the crimes noted elsewhere in the data base, facilities that were attacked were not well protected. The targets were only lightly defended, and the guards had a restricted capacity for armed defense. By contrast, in the commando raids, the targets were defended by personnel appropriately trained and equipped. Examining commando raids thus provides some insights into what strategies seemed most effective in attacking such facilities. At the same time, it must be noted that
these commando raids all occurred during wartime or severe civil strife, conditions that are not contemporarily extant in the United States. For this reason, the applicability of the commando analog to safeguarding nuclear facilities is limited as long as peacetime conditions prevail.

In reviewing the 75 commando raids, the success of the missions appeared to depend on three critical elements. The first was accurate information about the facility and its defenses. When accurate intelligence was lacking or misused, the mission almost always failed in its primary objectives, and often with the accompanying loss of the commandos. For example, over sixty British commandos, tasked to assassinate German Field Marshal Rommel, were safely landed in Libya in 1941. They successfully located and assaulted the complex where they had been told he would be, only to learn that he was with his troops. However, by attacking the building, they alerted German security forces, and only two members of the raiding party survived to rendezvous with their submarine. Similarly, outdated American intelligence resulted in the failure of the United States to rescue its P.O.W.s during the 1970 raid on the Son Tay prison camp in North Vietnam. In contrast, precise intelligence permitted a handful of Spanish loyalists to gain access to and destroy a Nationalist ammunition dump.

A second critical element contributing to the success of commando raids was careful planning. The destruction of eleven bridges in a single night by the Palmach was a textbook example of thorough planning and precise execution. Planning was essential to the success of British commandos who were able to overcome German defenders and spirit away an entire German radar facility from Bruneval during World War II. Israeli commandos have since accomplished similar acts against Egyptian radar sites.

The third critical element was surprise. In the cases in hand, the advantage of surprise was the decisive difference in determining the success or failure of a mission. Eighty-seven German glider troops surprised and captured a Belgian fortress and its 780-man garrison within a few hours when the German general staff had estimated that a conventional assault might require up to 6 months; similarly, 118
Germans rescued Mussolini from 250 troops even though several of the
German gliders crashed. Seven British commandos destroyed the German
heavy-water facilities in Norway, largely because the German defenders
thought the plant to be unassailable. Operations that proved to be
successful once could not be duplicated because a second attack, how-
ever well planned, lacked the advantage of surprise. For instance,
during the Second World War, German frogmen were able to destroy the
Nymwegen bridge in Holland with floating torpedo mines; when the
identical tactic was tried 6 months later against the Remagen bridge,
the defenders—no longer surprised by the tactic—killed or captured
all the German frogmen before they could accomplish their mission.

The critical variables here are more those reflecting human at-
tributes (such as dedication, ingenuity, intelligence) than the numbers
of men or material resources. There seems to have been little correla-
tion between the size of the commando group and its success in achiev-
ing its objectives. Indeed, one of the major tenets of the British
Special Air Services in North Africa was that a few men had a higher
probability of infiltrating and destroying their targets than a larger
number. Anticipating the targets to be well defended, the commandos
themselves were well armed. However, the quantity and quality of
weapons and munitions brought to bear seemed to have little influence
on the outcome of the encounter. The commandos were often able to
inflict devastating destruction with relatively simple weapons and
means such as mortars and sapper personnel.

In brief, the commando raids in the data base were coded as suc-
cessful 76 percent of the time; if one excludes those cases in which
the commandos' own shortcomings (such as faulty intelligence or me-
chanical breakdowns) resulted in the failure of their mission (i.e.,
the raid was not defeated by enemy defenders or defenses), the per-
centage of successes rises to 89 percent. A well-planned and well-
executed assault, characterized by imagination on the part of the
attacker and the advantage of surprise, has almost always succeeded,
even in the face of well-armed, trained defenders and formidable
physical barriers.
INDUSTRIAL SABOTAGE

Sabotage against industrial establishments, transportation facilities, and public utilities provides an obvious analog to potential attacks on nuclear facilities. As the term is used here, sabotage comprises acts of deliberate destruction, ranging from simple vandalism to efforts to inflict debilitating damage that would severely disrupt operations, disable a facility, and possibly endanger the public. We exclude deliberate slowdowns by workers or other forms of work interruptions or delay and acts of wartime sabotage.

The examination of sabotage is relevant to this study because it is a mode of adversarial action that could be used against and endanger U.S. nuclear programs. Sabotage has been a proven means of inflicting crippling damage, thereby bringing about work stoppages while arousing public concern. Typically, sabotage has involved persons who were employed by the sabotaged institution or who had inside knowledge of its design and operations, a condition that is of special concern for those designing safeguard measures for U.S. nuclear facilities and materials.

It is difficult to determine precisely how much of a problem industrial sabotage is in the United States. Many acts of sabotage go unreported; in some cases, it may be difficult to determine that an act of sabotage has occurred. A possible sabotage incident may be reported as an accident or employee negligence (e.g., a valve left open or a fire of unknown origin) or go unreported to avoid publicity or inspiring similar acts. In peacetime, few major incidents are known to have occurred, a conclusion reached by the authors of a report on the potential hazard of industrial sabotage in nuclear power plants prepared for the Atomic Energy Commission in 1968.*

The data base for our report contains 40 incidents of sabotage. Although most were single, isolated incidents, a few were part of a campaign of sabotage carried on over a period of time, such as four

separate train derailments during an extended strike against the Florida East Coast Railway in 1963-1964. The incidents examined here include a variety of acts, such as blowing up oil wells, severing power transmission lines, destroying newspaper printing presses, opening storage-tank valves to release petroleum products into the ocean, spilling gasoline into a sewer system and igniting it, and jamming a television station's transmission by interfering with its microwave relay tower (using the simple but ingenious expedient of sticking metal scoring pads on the surface of the metal dish). Explosive charges, arson, rifles, and various instruments simply thrown into machinery were among the means employed. Explosives were used in about half of the incidents.

The perpetrators of the sabotage incidents had such diverse characteristics that it is difficult to generalize about them or their motives. More than a third of the incidents, and the most serious ones, were committed by disgruntled employees or strikers. An additional 10 incidents involved persons who can be described as political extremists. The remainder involved foreign agents (for instance, in 1956, Egyptian saboteurs set fire to British oil wells in Libya), hired arsonists, extortionists, or disaffected, angry individuals. In about a sixth of the cases, the saboteurs remained unidentified. In most of the incidents in which the number of perpetrators was known, the act was carried out by a single individual; 9 cases were known to have involved six or more persons. Most of the latter incidents were carried out by groups of employees, people who knew each other because they had previously worked together.

In some cases, acts of sabotage appeared to have been relatively extemporaneous, as when strikers at a printing plant destroyed the presses as the workers walked off the job. In others, the sabotage was seemingly the result of thorough planning and careful execution. Motives underlying acts of sabotage included economic concessions (as in the case of striking workers), extortion, personal animosity or revenge, opposition to the "Establishment," and an insurance fraud. In the last case, a band of armed assailants, hired by the company's owner, entered a factory, disarmed the guards, and set off explosive
and incendiary devices. They posed as political extremists to cover their real reason for destroying the plant. Wartime sabotage directed against defense plants and shipping has been excluded from study. However, there are several incidents in which opposition to the Vietnam War was the explicit motive and several more in which it was the apparent motive. Many questions as to motives remain unanswered.

For the most part, the saboteurs selected undefended targets, such as rail lines, transmission towers, relay stations, and power lines that did not require their penetration into guarded facilities. Most of the targets struck were located in remote areas. In only a few incidents did the perpetrators illegally enter the facility they were planning to damage. (The 1968 AEC report cited above makes the same observation.) Employees, of course, would have legitimate access. In only one incident did the saboteurs confront and disarm security guards; this occurred in a case of sabotage for purposes of insurance fraud.

Weapons generally were in little evidence in the incidents examined here; they simply were not needed for the act. For the most part, the saboteurs relied on relatively simple techniques and, in many cases, on inside knowledge to carry out their actions. Their knowledge of the facility's operations and possibly restricted areas made them privy to the organization's critical, vulnerable areas, thus making their acts particularly effective given their limited resources. Their technical expertise also increased their effectiveness.

With a few exceptions—the derailment of trains, for example—the saboteurs did not deliberately endanger the lives of others. The actions carried out by the saboteurs required them to take few risks. Their disproportionately high effectiveness (in terms of accomplishing their objectives), which was achieved by a few people with minimal means (in one case, literally a few bolts) and at low personal risk, was largely the result of access to accurate inside information and restricted areas.

**SYMBOLIC BOMBINGS**

For purposes of this study, "symbolic bombings" are defined as deliberate acts of violence calculated to express a grievance or make
a political statement. The target is perceived by the adversaries as having symbolic significance for their cause. The damage to the target may be secondary, or even irrelevant, to the adversary's aims.

The study of symbolic bombings is applicable to potential future nuclear incidents because nuclear facilities are viewed by some as symbols of unwarranted and dangerous technology. Indeed, nuclear installations have already been subjected to a number of symbolic bombings in the United States and abroad.

The database currently contains 110 incidents of symbolic bombing in the United States that occurred between 1965 and 1976. The targets were about evenly divided between commercial facilities (such as corporate headquarters and banks) and government buildings (such as embassies and police stations). A few residences were also targets.

Symbolic bombers were generally motivated by political extremism, opposition to the activities of particular corporations, and anger at public officials or the acts of public agencies. In 1975, the Weather Underground claimed credit for an explosion at the Department of State building in Washington, D.C. A group calling itself the "Anti-Establishment Revolutionary" claimed credit for the bombings of the Chase Manhattan Bank, Standard Oil of New Jersey, and General Motors, all in late 1969. In 1970, "Revolutionary Women" firebombed the home of a police commissioner in New York City. Even though symbolic bombings were usually not intended to kill people, one bomb, clearly intended to kill people, was detonated in the Fraunces Tavern on Wall Street during the lunch hour, killing 4 and injuring 55; total casualties of the bombings in the database were 4 dead and 69 injured. The Lawrence Radiation Laboratory, the Stanford Linear Accelerator, and the French nuclear generating station in Brittany have all been the targets of multiple bombings.

Although motives are not always clear or easily identifiable, damage for symbolic reasons appeared to have been a significant consideration. Most bombs were planted by stealth and exploded at night. Although the bombings were largely planned by extremist groups, the acts themselves were usually carried out by only a few individuals. Left-wing revolutionary groups--such as the Weather Underground, Red
Guerrilla Family, and the New World Liberation Front—seemed to predominate.

None of the incidents studied required a great deal of advanced planning, although most required at least a moderate amount of prior reconnaissance of the target. The bombers looked for "soft" (i.e., unprotected) targets that had little or no security system. There is no evidence that the adversaries in any of the incidents examined had inside knowledge or privileged information beyond that which would be available from public sources and from observation of the intended targets. Targets, at times, seemed to have been selected partially on the basis of convenience. While the symbolic bombers, by virtue of their actions, must be classified as dedicated to their cause, there appears, at the same time, to be an element of caprice and a degree of casualness in carrying out the bombings; the bombers displayed a minimal expenditure of energy and a minimal exposure to risk in carrying out their symbolic acts.

In most cases, no special equipment was needed in placing or transporting the devices used. Some of the bombs were crudely made; the explosives were easily obtained either by purchase or theft, and required little more than a knowledge of explosives gained by a cursory reading of any of the many publicly available manuals on the market. Some bombings, however, were far more sophisticated and indicated a much higher degree of expertise, intelligence, and care. For instance, some of the bombings claimed by Puerto Rican separatists showed evidence of considerable skill in the design and placement of the explosives.

In summary, for symbolic bombings, the aim was usually abstract—an institution, a condition, or a policy rather than a particular physical target or facility. A symbolic bombing was fundamentally a protest action, chosen because it was a relatively safe, available, and apparently satisfying way for the bombers to express themselves.

NUCLEAR INCIDENTS

As stated earlier, known incidents regarding nuclear facilities and materials have been included as part of the data base. These are
not, of course, analogs; rather they are actual nuclear incidents. They are included to illustrate the range of threats and incidents that have occurred to date involving nuclear programs.

Between 1969 and 1975, there were 288 recorded threats against, or incidents at, nuclear facilities in the United States. The majority of these (240) were bomb threats against government or licensed nuclear facilities. Twenty-two were incidents of arson, attempted arson, or suspicious fires. Most of the apparent arsons occurred in buildings where the Atomic Energy Commission rented offices or were directed against university research facilities, such as the University of California's Lawrence Radiation Laboratory. The Lawrence Laboratory was a frequent target; 10 arson incidents and 5 bomb threats were recorded there. Investigators suspect that the incidents were created either by former employees with personal grievances or militant students opposed to nuclear research being conducted at the university.

The most serious incident of arson occurred at a nuclear generating plant at Indian Point, New York. In November 1971, a fire caused $10 million in damage to the facility, but did not affect the reactor. A subsequent letter to the press claimed that "Indian Point guerrillas" were responsible for the incident and suggested that the action had been motivated by concern for the environment. The arsonist, who was later apprehended when he turned himself in for psychiatric treatment at a local veterans hospital, turned out to be a former employee of the company.

There were 9 bombings in the database. In one episode, the target clearly was a nuclear program. In December 1971, two bombs exploded near the experimental linear accelerator at Stanford University in California, causing heavy damage to the electronics equipment that controls the facility. A caller later claimed credit for the explosions, but no manifestos were issued and no suspects were ever arrested. The remaining bombs exploded at federal office buildings or university research facilities, but it is not clear if nuclear programs were the target. In addition, there were 4 incidents in which unexploded bombs or explosives were discovered at nuclear facilities. Again, research facilities were the principal target.
In February 1974, an opponent of nuclear power toppled a 400-foot meteorological instrument tower at a proposed nuclear power plant site in Massachusetts. The perpetrator, who surrendered himself to police, claimed in a written statement that his action was motivated by opposition to the future construction of a nuclear power plant at the site and to the danger this would impose on the community.

The remaining incidents consist of forced entries, intrusions, shots fired at guards or at transmission towers, or malicious mischief. In one incident, a college student cut through a fence to gain access to the area around a university research reactor, later stating he had done this simply to prove that it could be done.

A widely publicized incident involving the removal of nuclear material occurred at a fuel fabrication plant in Oklahoma. Controversy still surrounds this case. On the basis of two government reports and various press accounts, it appears that in November 1974, a plant employee, who had previously complained that working conditions at the plant were unsafe, was found to have been contaminated with plutonium and placed on administrative duties. When routinely checked the following day, she was again found to be contaminated. A further check of her apartment also revealed some contamination. She died in an automobile crash 8 days after the first incident. Her autopsy revealed radioactive contamination but not at the higher levels found before her death, which suggests that earlier samples may have been deliberately contaminated. At the same facility a month later, uranium dioxide pellets were found lying on the ground outside the production area. There was no way they could have gotten there accidentally. A plant employee who may have wished to embarrass the company was suspected. While neither incident involved significant quantities of nuclear material, they did raise serious questions about the security of the facility and the possibilities of a more serious diversion.

None of these incidents, with the possible exception of the fires at the Lawrence Radiation Laboratory and the Indian Point nuclear power plant and the bombing of the Stanford linear accelerator, imperiled public safety. There was only one casualty, which occurred when an intruder entering a nuclear power plant in Vermont wounded a night
watchman. The remainder of the nuclear incidents that occurred in the United States could be classified as minor, such as bomb threats, token acts of violence, and low-level sabotage. Many incidents were directed against only administration facilities—e.g., office buildings, campus science buildings—connected with nuclear programs.

In addition to the 288 incidents mentioned above, several known thefts of radioactive material or devices containing radioactive material have taken place at facilities and institutions not defined as "nuclear facilities." For example, in August 1973, twenty-one capsules of radioactive Iodine-131 were stolen from a hospital in California. In June 1974, an instrument containing Strontium-90, which was used to measure the density of railroad beds, was stolen. The following year, nine radioactive radium needles were stolen from a hospital in California by a night porter who worked at the hospital. It has been reported that burglars involved in these thefts may not always know what they are stealing and may have disposed of the instruments or materials when they were found not to be marketable.

There is no complete record of incidents involving nuclear facilities or material elsewhere in the world. From the reports of the incidents that are known to have occurred, they do not differ markedly from those in the United States and consist mainly of bomb threats, hoaxes, incidents of vandalism, and low-level sabotage. In the last few years, however, several more serious incidents have taken place.

In May 1975, two bombs exploded at a nuclear power station under construction in Fessenheim, France. The explosions started a fire that damaged a peripheral area of the nuclear reactor complex. The reactor itself did not yet contain fissionable material. Shortly before the bombs exploded, a caller identified himself as a member of an unknown group that took its name from two known anarchists. In the months preceding the bombing, there had been local opposition to the construction of nuclear power stations in the area, so it was reported that antinuclear extremists may have used the cover of political extremism to publicize their cause. Two bombs were detonated at other French nuclear facilities in June 1975. Again, a previously unknown group claimed credit for the incidents. One bomb was placed at
Framatome's main computer center in Courbevoie, destroying half of the input terminals; the second bomb was planted at Framatome's workshop in Argenteuil, causing some damage in the valve-testing shops. Again, it was speculated that persons opposed to nuclear power may have been using a political cover to advance their cause.

In August 1975, two bombs exploded at a nuclear power plant in Brittany, France. The bombs caused minor damage to an inlet for cooling water for the reactor and to an air vent on the building on the power station. The reactor itself was not damaged, but was closed down pending an investigation. No one claimed responsibility for the attack, but police suspected that it had been carried out by a Breton separatist group responsible for other recent acts of sabotage in the area.

In early November 1976, a bomb was exploded in the Paris offices of a manufacturer of nuclear fuel elements. The blast caused extensive damage but no casualties. Responsibility for the attack was claimed by a man identifying himself as a member of the Commando d'Opposition par Explosifs a l'auto-destruction de l'univers ("Commando of Opposition by Explosives to the Self-Destruction of the Universe"), forming the French acronym COPEAU. Less than a week after the Paris blast, COPEAU claimed credit for two bombs detonated at a uranium mine in southwestern France. The bombs destroyed four pump compressors, putting the mine out of operation for about 2 months and causing an estimated $2 million damage.

In Sweden, where nuclear power has met similar resistance, 44 pounds of dynamite were found next to a nuclear power station at Ringhals in November 1976. The bomb, defused by police, would have damaged transformers but not the two reactors.

Several serious incidents of theft have occurred abroad. In November 1966, twenty uranium fuel elements containing slightly enriched uranium were stolen from the Bradwell nuclear power station in Great Britain. The theft was carried out by two men (one an employee at the plant) who were later arrested; the fuel elements were recovered. The thieves said that a man in London had offered them money for the elements, but the London connection was never identified.

In April 1974, a uranium-smuggling operation in India was exposed.
Complete details of the incident are not available, but it appears from the rather sketchy press accounts that natural uranium was being removed from a plant in Bihar, India, and smuggled to Nepal. From Nepal, it was secretly shipped to Hong Kong where, reportedly, Chinese or Pakistani agents took delivery. It is suspected that as much as $2.5 million worth of uranium may have been involved. The plot came to public attention when five persons involved in the operation were arrested in India and 3.5 kilograms of uranium were recovered.

There have been 2 incidents abroad involving the use of radioactive material as contaminants. In April 1974, an anonymous caller in Austria warned that some train coaches had been deliberately contaminated with radioactive material. Investigators found substantial but not lethal traces of Iodine-131, a radioactive material normally used for medical diagnosis. The episode received widespread publicity in Austria and provoked a number of hoax calls and threats. The perpetrator, who was later arrested, turned out to have a history of mental illness. He had intended his actions to be a protest against the treatment of the mentally disturbed in Austria.

In October 1974, Italian government officials announced that they had discovered a plot by right-wing terrorists to poison Italy's aqueducts with radioactive waste material stolen from a nuclear research center in Northern Italy. The alleged threat was associated with revelations of a planned assassination and political coup by right-wing elements. An engineer at the research center was named as a conspirator, but the allegations were never substantiated. The case became entangled in legal technicalities. Whether the alleged plot, which gained widespread publicity in Italy, was real or not has never been determined.

A single nuclear incident is known to have taken place in Latin America. In March 1973, fifteen members of a leftist urban guerrilla group in Argentina occupied an atomic power plant under construction at Atucha, 62 miles north of Buenos Aires. They overpowered the guards, painted slogans on the walls, raised their flag over the facility, and stole weapons, but they made no demands and did not attempt to enter the reactor area or damage the facility.
What might we conclude from these nuclear incidents? For the most part, public safety was not imperiled. Like other businesses and industries, the nuclear industry is also susceptible to bomb threats, arson, incidents of low-level sabotage, and occasional bombings. Only a few incidents attracted widespread attention. The perpetrators and their motives were diverse. They included disgruntled employees, common thieves, political extremists, foes of nuclear power, and a few lunatics; their apparent motives included protest, greed, revenge, or desire for attention. The culprits included insiders, external groups, and combinations of both. For the most part, however, they were probably acting alone; only a few incidents involved groups. There is no evidence in the incidents that any criminal or terrorist group has made any attempt to acquire special nuclear material or radioactive waste for use in an explosive or dispersal device. No individual or group has yet demonstrated such a capacity.
IV. ANALYSIS OF THE DATA BASE

The formal data base used for this report has been structured in such a manner that it compares the five types of incidents—task force crimes or "capers," commando raids, industrial sabotage, terrorist assaults, and symbolic bombings—with respect to a number of key attributes observed in each. This will allow us to aggregate and examine acts of criminal and political violence from the perspective of the various attributes; it represents a "horizontal" aggregation of the data. Later, "typical" adversary acts and typical composite, high-level composite adversaries ("vertical" aggregation) will be constructed. The percentages shown below are computed within each category of analogs based on a total of 45 capers, 34 assaults, 110 bombings, 75 commando raids, and 40 incidents of industrial sabotage. As noted above, incidents involving nuclear materials or facilities are not included here.

CLASSIFICATION AND CODING

Rand and Sandia personnel jointly designed a Threat Characteristics Outline to provide a framework within which these five types of incidents could be coded on a standardized basis. (This outline is reproduced as Appendix A.) Some incidents fit this framework rather awkwardly. Furthermore, full information for all the incidents was not available, and judgmental choices were necessary in coding the incidents. For these reasons, and to preclude the possibility that the data will be misinterpreted, it is advised that the data presented here not be taken out of the context in which they are presented.

*The percentages within a category do not add to 100 percent for all attributes. There are some attributes for which more than one answer applies in particular incidents—for example, in some cases access to a target may have been gained by disabling an alarm and barrier penetration—resulting in totals greater than 100 percent. There are others for which no category applies—e.g., assaults in which the perpetrator surrendered and no attempt at egress was made—giving totals less than 100 percent.
Aims and Objectives

Adversaries' aims are considered first. The perpetrators of all the terrorist assaults and bombings are best classified as political extremists with political aims in mind, whereas most of the capers were carried out by criminals whose primary aim was personal financial gain. For the present purposes of classification, the Palmach and Viet Cong commando raids have been considered as having been executed by political extremists, although they carried some of the trappings of national legitimacy.

The objectives for the incidents follow anticipated lines. The tactical objective in all the symbolic bombings appeared to be at least token damage with the aim of disrupting the facility attacked and, in most cases, publicity for a cause. Political demands were made in a few of the bombings, but probably without serious expectation that the demands would be met. In about 90 percent of the capers, the immediate objective was theft; the remainder of the capers were prison breaks, coded as an objective of "disable/disrupt." About 80 percent of the assaults by terrorists were intended to seize and hold a facility with hostages in return for political concessions, and about 30 percent had the objective of creating damage and disabling or disrupting the facility attacked; 10 percent involved both. Over 90 percent of the military commando raids were directed toward the disruption or destruction of the enemy's war-fighting capabilities; the remainder were planned rescues of personnel. Personal anger was undoubtedly a factor in many of the assaults and bombings, but was only clearly identifiable as an important secondary motive in a few cases. In three-quarters of the cases of industrial sabotage, destruction of facilities was identified as the principal objective.

Number of Adversaries

Excluding the military operations, the most frequent number of adversaries observed ranged between two and five persons, with one criminal caper and a terrorist assault carried out by a lone individual.

These terms as we have used them are defined in Appendix B.
Roughly a quarter of the capers and a third of the terrorist assaults involved six or more people. The largest caper involved about twenty men; the largest terrorist assault raid involved a group of thirty. The average number of men in commando raids was slightly less than thirty, although several successful raids were conducted by fewer than a dozen men. The estimate of participants in most symbolic bombings was between two and five; this represents a "best guess" or default value because the limited hard data available for this category suggest the low number. Many of the bombs could actually have been placed by one person, although the bombings all appeared to have been planned by groups, rather than by lone individuals. Testimony taken from apprehended bombers indicated that the involvement of two persons—one planting the bomb and the other acting as a lookout—was the mode generally used. Two to five adversaries were also assumed for some of the burglaries in which knowledge of the number of perpetrators was uncertain. The distribution was relatively bimodal for industrial sabotage incidents in which the number of adversaries could be identified; over 40 percent were carried out by a solitary individual while another 25 percent were executed by six or more persons.

The number of perpetrators in all categories—more specifically, the small numbers seen in many of these incidents—appears to have been determined more by operational requirements than by any resource limitations. Most of the assaults and bombings were carried out by groups that potentially had more people available than were actually employed for the given operation.

**Armament and Equipment**

To the best of our information, no weapons were employed in the bombings (except one), in most of the sabotage incidents, or in most of the capers (such as burglaries). This does not mean that the perpetrators in these cases were unarmed, but rather that they simply had no need to display or use weapons. Most of the armed robberies involved commercially available pistols and shotguns. Submachine guns were used in one case, a crew-served heavy machine gun in another, and an antitank gun was used in a third one (but, in this study, the
last is classified as a "special tool" rather than a weapon, because it was used solely to penetrate a vault). One of the terrorist assaults was made with pistols, whereas the rest were accomplished with automatic weapons and grenades; in several cases the attackers carried explosives as well. The armament employed in some of the commando raids included light crew-served weapons, such as recoilless rifles and mortars.

Turning to the equipment used by the adversaries, one finds a strong correlation between the different types of incidents and the particular equipment brought to bear. Obviously, explosives (including incendiary devices) were used in all the bombings and, in most bombings, were the only "tools" employed. In half of the cases of industrial sabotage, special tools or explosives were used, whereas the remaining incidents were characterized by the use of hand or power tools. No tools were employed in the terrorist assault cases, with one exception in which wire cutters were used to cut through a fence. The military commandos used a full complement of tools and equipment ranging from wire cutters to advanced electronic equipment. In some cases, special equipment was designed to meet specific needs.

As a function of equipment used, the capers may be divided fairly evenly between the three categories: no tools, relatively standard equipment, and very specialized implements. Those capers involving no tools were primarily armed robberies. In the second category, tools and equipment used in burglaries included crowbars, drills, sledgehammers, cutting torches, and explosives. In one case a truck-mounted hoist was used. In the third category, specialized electronics equipment was employed to defeat alarm systems in a number of cases. Communications equipment used by burglars and robbers included radios and wire field telephones. Sophisticated penetration devices included thermic rods. Helicopters were used to fly prisoners out of prison yards in two instances; in one case, the helicopter was rented and abandoned; in the other, it was chartered and the pilot was subsequently coerced at knifepoint.

Access and Egress

In virtually every bombing case, access to the target area or the target itself was accomplished either by legitimate means—e.g., by
entering an area open to the public—or by deception—e.g., gaining entry to an accessible but closed-to-the-public area. Neither tactic required the use of force. Two exceptions involved the penetration of light barriers, such as chain link fences. All the burglaries, and some of the robberies, assaults, and sabotage, involved forced entry of some type. This forced-entry characteristic should not be surprising, because the targeted facilities were designed to prevent unauthorized access. Legitimate access and deception were often combined in practice. However, for coding purposes, it may be impossible to separate them after the fact. For example, when a bomb is left in a corporate restroom, it cannot be retrospectively determined whether the bomb was placed by someone acting as an ordinary member of the public (i.e., legitimate access) or by someone posing as a delivery boy (i.e., deceit or deception).

About 15 percent of the terrorist assaults involved some form of barrier penetration or barrier bypass, and almost half of them, some form of "legitimate" access. The barrier penetrations included such acts as cutting through fences and scaling walls. In the "legitimate" accesses, the culprits overtly entered the target facility (e.g., an airport or embassy) as peaceful members of the public, and then drew their guns and began the assault after they were inside. The line between access gained by legitimate means coupled with armed assault and pure armed-assault access is obviously fuzzy, with the coding depending in part on how the incident was described in the case study. The primary methods of facility access in the capers were armed assault for armed robberies and covert barrier penetration for burglaries and prison breaks. Legitimate access or deception (e.g., crooks posing as burglar-alarm repairmen) was employed in about one-third of the capers.

Once the adversaries had gained entry, their tactics were largely dependent on their original objectives and the response of the defensive system. Theft was involved in 90 percent of the capers (all but the prison breaks), but happened in only one of the terrorist assaults and in none of the symbolic bombings. The occupation of a facility and the holding of hostages within it occurred in 80 percent of the terrorist assaults and in slightly more than a third of the capers, but in none
of the incidents of sabotage, commando raids, or symbolic bombings. (The capers in this case were armed robberies in which the facility was held briefly while the robbery took place. "Holding" in the case of capers is thus quite different from "holding" in the terrorist assaults.) The creation of physical damage, per se, was intended or occurred in about a third of the assaults and in all but one bombing. Over 90 percent of the commando raids were planned with the physical destruction of targets as the primary objective; the only exceptions were 5 raids to rescue prisoners and 2 raids to obtain enemy radar sets.

The method of "egress" from the target following the incident—i.e., the adversary's means of escape after he has accomplished his primary objectives—varied according to the activity. The symbolic bombs were all planted by persons employing stealth or deceit; hence, this was the form of egress in all the bombing incidents reported. In 80 percent of the assaults, the perpetrators attempted to bargain their way to safety, although not always successfully, and in two incidents, they outran the response. In the remaining assault incidents, no egress was attempted; the perpetrators either surrendered or were killed before any attempt at bargaining or other avenue of escape could be instituted. The capers were about evenly divided between stealth—which was used for most burglaries—and attempts to outrun the response—which occurred in armed robberies, prison breaks, and some burglaries. In close to 90 percent of the incidents of industrial sabotage, the perpetrators escaped either by stealth or by outrunning the system's response mechanisms. With the exception of the seemingly suicidal Viet Cong attack on the U.S. Embassy in Saigon, commandos also favored stealth or outrunning the response, although in many cases an armed retreat was necessary.

**Duration**

The time necessary to conduct any of these operations is an important characteristic of the action. We do not have complete information on the time required to execute all the incidents in the database. Those for which we do have information indicate that such operations can be executed with remarkable speed. The slowest events to unfold
were burglaries in which the burglars were forced to penetrate strong physical barriers, such as stationary bank vaults; such operations usually required between 5 and 10 hours. When the burglars were able to use deception or inside assistance to gain entry to a secured area, or managed to obtain keys and combinations to gain access to a vault, the crimes took less than 10 minutes. Armed robberies were often carried out with remarkable speed. The famous Brinks' robbery in Boston was carried out in less than 20 minutes, including the time needed to load a million dollars in cash. Speed, of course, is a necessary characteristic of a commando raid. Likewise, terrorist assaults are carried out with great expedition. The time involved in bombing is irrelevant, since the bomb is planted at the adversaries' convenience and later detonated by a timing device. Similar logic is applicable in cases of industrial sabotage. Thus, one can credit the adversary with the ability to carry out whatever action is contemplated in a relatively short time.

PROFILES

We have drawn on the data base to examine the various adversary attributes, such as numbers, equipment, arms, transportation, intelligence, dedication, aims and objectives, training, imagination, and ingenuity that have characterized these actions and their perpetrators. (A list of adversary attributes appears in Appendix C.) In addition, aggregate profiles of "typical" actions in each category can be compiled from the data base. It is important to realize that the following profiles are composites; as with any composite representation, individual cases will vary from the profile. However, the profiles do represent "typical" cases of each category of analogs and are exemplary of real-life actions. In most cases, the capabilities displayed by the adversaries were sufficient to achieve their desired objective. They do not manifest the upper limits of the resources available to the perpetrators involved. Rather, they represent the baseline capabilities commonly found in the various categories of successful crime and politically motivated violence examined here.
"Typical" Analog Profiles

A "typical" terrorist assault team consisted of three to six men armed with automatic weapons, grenades, and explosives. They were trained, although not extensively, in the use of weapons, explosives, and elementary tactics. They were sufficiently dedicated to their cause to accept a high risk of capture or death. They were not likely to possess extensive technical skills, but in most cases, such skills were not a requisite to the success of the mission. Their transportation included cars, trucks, boats, aircraft, or movement on foot, basically whatever was required to arrive at a given target. Their objectives ranged from seizing and holding a facility and its occupants as hostages in exchange for political concessions to attacking a facility or people. The operations normally were conceived and planned by a larger organization, i.e., a "parent" group with sufficient resources to support extensive intelligence collection, planning, and training. The degree of imagination and ingenuity shown in such operations ranged from moderate to high.

A "typical" burglary task force consisted of two to four men. The men were professional criminals,* they were both skillful and careful. One of them was likely to be an expert in overcoming complex electronic alarm systems. Their intention was to obtain maximum profits with minimum risks and their motivation was economic gain; their target was usually cash or high-value merchandise that was relatively easy to dispose of. To these ends, the tools, explosives, and the special equipment necessary to penetrate significant physical barriers of steel and reinforced concrete and to neutralize alarm systems were readily available. Transportation was by automobile, truck, and occasionally aircraft, depending on the size and weight of the loot. Burglars often had inside information (particularly concerning the alarm system and routines of any guard force), and usually surveyed the target area carefully while planning the job. They were armed, but generally did not

*We do not mean that they were necessarily a part of organized crime, but that they were professional in the sense that they had experience and expertise in these types of activities and had made their living primarily in this fashion.
use their weapons, seeking to avoid confrontation with security forces rather than to prevail by force of arms.

The members of the task force were carefully selected, as much for their trustworthiness and reliability as for their specific job skills, because they had to be trusted not to reveal the group or its plans, either before or after the operation, even if apprehended. Characteristically, they planned carefully, estimated their chances of success, and took every precaution to minimize risks. Thus, the "typical" caper group may have rehearsed its operation many times to enhance its chances of success. Group members may actually have scheduled the theft several times but delayed their caper because they sensed that their chances for success were in some ways significantly compromised. The degree of imagination and ingenuity shown was quite high.

A "typical" sophisticated armed robbery team consisted of three to six men. Robbers were usually professional criminals who were possibly less skilled (or their crimes may simply require fewer skills) and somewhat less averse to taking risks than burglars. They were sufficiently well armed—generally with handguns and shotguns that were clearly visible—to give them a substantial advantage over anticipated security forces. The criminal team preferred to avoid violence but was willing to display weapons and, when necessary, to use them. The display of superior force was to discourage possible resistance and a potential shootout. Transportation was via car or light truck. As in the typical burglary, the target was usually cash or high-value merchandise or material in a facility, or possibly in transit. The degree of planning was usually moderate, but occasionally very extensive. Some inside knowledge, particularly about shipment schedules and security, was frequently used. The degree of imagination and ingenuity displayed varied but, on occasion, was high.

A "typical" symbolic bombing was politically motivated. It usually involved the planting of dynamite, or other explosive with a timing device, in a government building or corporate headquarters. The evidence suggests that only one or two people generally participated in the actual planting of the bomb, but others may have been involved in planning, building the bomb, and other related activities. The
total membership of the larger group appears to have ranged from ten to thirty. For the most part, the perpetrators seemed to have been largely self-trained through publicly available literature on guerrilla warfare and explosives; they were moderately skillful in the design and fabrication of the devices. The bombers were characterized by strong but volatile loyalty and dedication, floating in and out of a number of sympathetic groups. Their transportation included cars, light trucks, and public transit. The targets were chosen for high political impact at minimum risk to the group. Few attempts were made to confront a significant security system. The imagination and ingenuity were only moderate, possibly because only a moderate amount of ingenuity was generally required. The target was usually property, not people; indeed, attempts were often made to avoid casualties. The explosives in most cases were set to explode at night, usually preceded by telephone warnings to the building, the news media, and/or the police.

The explosions in symbolic bombings were frequently followed by a written communiqué. The aim of the bombing, often stated in an accompanying communiqué, was to make a political statement, possibly related to some current or recent political events. The communiqué was a critical element in the bombing; it provided the perpetrators with access to the media and the opportunity to "educate" the public to their cause. Planning and preparation prior to the emplacement of the bomb were often extensive, partly because the planning exercise itself was an important social and political activity for the political activist group.

The commando raids were conducted by professional soldiers or guerrillas who were, generally speaking, highly skilled and specially trained for their duties. Their aims were the disruption of the enemy's war-fighting capabilities, with the noted exception of those missions to obtain enemy equipment or to rescue captured comrades. The men were highly motivated, undertaking actions that often came close to being suicidal and occasionally extracted a heavy toll of life. Prior planning was often extensive, including practice raids on mock facilities in a few cases. Intelligence information, when erroneous, almost always defeated the purpose of the mission.
It is important to note that commando raids were carried out against protected targets whose defenders usually outnumbered the raiders and were at least as well armed as the commandos, conditions that would hardly seem to bode well for the raiders. Yet, with the advantages of greater flexibility and tactical surprise, the raids succeeded three-fourths of the time and against some targets whose defenses could have prevailed against much larger forces; if one excludes those failures that were not due to enemy action, the commandos were successful almost 90 percent of the time. This rate of success speaks highly for the professional skill and ingenuity of the raiders, and particularly for their use of surprise. (It also bodes ill for the use of mathematical engagement models in which force ratios determine the outcome.)

A "typical" incident of industrial sabotage was either carried out by a solitary person or a group of more than six. Approximately a third of these cases were attributed to political extremists, and another third were attributed to disgruntled persons. Their objectives always centered around the destruction or disruption of facilities or equipment, quite often on a significant scale. They rarely appeared to have firearms. Their primary equipment was the material or tools of their chosen methods of sabotage. The saboteurs were sufficiently motivated to carry out their acts but generally chose those that did not require them to take extreme risks, such as being confronted or captured.

The saboteurs used conventional means of transportation. Perhaps the critical characteristic is that they generally had inside contacts or privileged information not available to the general public. This gave them relatively easy access to their selected targets, which—as they knew from their information—were invariably the critical or exposed points in the targeted facility. They were well trained, if not in techniques of destruction, then in the workings of the facility so that they could effectively disable it.

A major difference between incidents of industrial sabotage or burglaries/armed robberies and the rest of the categories is that the perpetrators of the former incidents usually had little desire to have their identities known or widely publicized; sabotage and crime are almost always carried out to satisfy individual objectives or personal
gain. The identification of the perpetrators hardly serves—indeed, defeats—their purposes. While political bombers and terrorists usually prefer to keep their individual identities secret, they publicize their group affiliation.

Typical Composite Profile

Table 2 summarizes the adversary attributes displayed in these six "typical" types of actions. We have further consolidated the attributes by creating a "typical composite profile," shown in Table 3. This latter profile is a compendium of the equipment, skills, and other attributes that have been brought to bear against the analog targets. It represents a level of resources and skills that criminal and political adversaries have been able to assemble and, as such, might be able to assemble were an adversary group to target a nuclear facility. (The typical composite profile does not include the commando raids.) A composite of the typical attributes seen in all categories of crimes surveyed consisted of three to six adversaries armed with automatic weapons, possessing high explosives and hand and power tools, using a variety of ground transportation modes, having high technical skills and a willingness to accept high risks, possessing some inside information or assistance, and displaying a moderate-to-high degree of ingenuity and careful advanced planning.

One must be extremely guarded in interpreting and applying this typical composite profile to the nuclear situation. What is presented as the typical composite profile is not an assessment or depiction of the potential adversary of U.S. nuclear programs. It is a description of attributes that have been frequently displayed by adversaries in other, analogous circumstances. Based for the most part on successful operations, the profiles show what attributes and characteristics the adversaries found were necessary to have a high probability of achieving their goals.

The typical composite profile represents a reference point on a scale of adversarial capabilities. This point has not been determined solely as a function of the resources available to criminals and terrorists, but also by what is required for their success, which, in turn,
<table>
<thead>
<tr>
<th>&quot;Typical&quot; Action</th>
<th>Number of Perpetrators</th>
<th>Weapons</th>
<th>Tools</th>
<th>Transport</th>
<th>Technical Skills</th>
<th>Dedication (willingness to risk death or capture)</th>
<th>Inside Assistance</th>
<th>Planning</th>
<th>Ingenuity and Imagination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorist assault</td>
<td>3-6</td>
<td>Handguns, automatic weapons</td>
<td>High explosives</td>
<td>Foot, commercial vehicles, air</td>
<td>Medium</td>
<td>High</td>
<td>No</td>
<td>Medium to high</td>
<td></td>
</tr>
<tr>
<td>Robbery</td>
<td>3-6</td>
<td>Handguns, shotguns</td>
<td>None</td>
<td>Foot, commercial vehicles</td>
<td>Medium</td>
<td>Medium</td>
<td>Information</td>
<td>Medium to high</td>
<td></td>
</tr>
<tr>
<td>Burglary</td>
<td>2-4</td>
<td>Weapons usually not displayed</td>
<td>Hand and power tools, high explosives</td>
<td>Foot, commercial vehicles</td>
<td>High</td>
<td>Low to medium</td>
<td>Information</td>
<td>High</td>
<td>Medium to high</td>
</tr>
<tr>
<td>Bombing</td>
<td>1-2</td>
<td>None</td>
<td>Hand and power tools, explosives</td>
<td>Foot, commercial vehicles</td>
<td>Low to medium</td>
<td>Low</td>
<td>No</td>
<td>Medium</td>
<td>Low to medium</td>
</tr>
<tr>
<td>Sabotage</td>
<td>2-5</td>
<td>Usually none</td>
<td>Hand and power tools, explosives</td>
<td>Foot, motor vehicles</td>
<td>Low to medium</td>
<td>Low</td>
<td>Information and access</td>
<td>Medium</td>
<td>Medium to high</td>
</tr>
<tr>
<td>Commando raid</td>
<td>20-30</td>
<td>Automatic and light crew-served weapons, explosives</td>
<td>Hand tools, explosives</td>
<td>Foot, air, ship, and motor vehicles</td>
<td>High</td>
<td>High</td>
<td>Information</td>
<td>Medium to high</td>
<td></td>
</tr>
<tr>
<td>Adversary</td>
<td>Number of Perpetrators</td>
<td>Weapons Used</td>
<td>Tools Used</td>
<td>Mode of Transportation</td>
<td>Technical Skills</td>
<td>Dedication (willingness to risk death or capture)</td>
<td>Inside Assistance</td>
<td>Planning</td>
<td>Ingenuity and Imagination</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------</td>
<td>----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>&quot;Typical&quot; composite</td>
<td>3-6</td>
<td>Automatic weapons, grenades, shotguns, explosives</td>
<td>High explosives, hand and power tools</td>
<td>Foot, commercial vehicles, limited use of aircraft</td>
<td>Medium to high</td>
<td>Medium to high</td>
<td>Information or other assistance from one insider</td>
<td>High</td>
<td>Medium to high</td>
</tr>
</tbody>
</table>
is determined by the level of societal tolerance for their successes. Armored express companies, banks, criminal justice agencies, insurance companies, and the society at large have, in effect, decided that the occasional criminal successes are not sufficiently damaging to warrant using the additional resources required to reduce substantially the occurrence of such crimes. In other words, society tolerates a certain number of criminal successes. If this were not so—i.e., if society were to demand their reduction—the resources required to carry out such crimes successfully would correspondingly increase. The demand for a reduction in airline hijacking, the resulting more stringent airport inspection measures, and the subsequent decrease in sky-jacking incidents are good examples of a change in societal tolerance of a type of criminal activity and of the increased resources dedicated to public safety demands. If society were to mandate a change in the public safety environment, the reference points would necessarily be altered.

The High-Level Composite Profile

Table 4 shows a "high-level composite" profile of adversary attributes and characteristics, which aggregates high-level attributes so far observed in real-life episodes, although not necessarily the highest levels seen. The choice of high but still plausible levels, based on the authors' judgments, seems clearly preferable to positing a more speculative adversary and his capabilities predicated on the highest levels observed.

The high-level composite helps to identify which capabilities are the hardest for an adversary to attain, and at what levels he begins to encounter difficulties. We refer to these levels as "breaking points." For example, our research indicates that in the mobilization of manpower and the acquisition of weapons, an adversary can in fact attain the high levels shown in Table 4. On the other hand, the recruitment of persons possessing specific technical skills who are also willing to risk their lives seems to pose somewhat of a greater obstacle.

The high-level composite provides another reference point on a scale of adversary capabilities, obviously much higher on the scale than the typical composite profile. If the typical composite profile
<table>
<thead>
<tr>
<th>Adversary</th>
<th>Number of Perpetrators</th>
<th>Weapons Used</th>
<th>Tools Used</th>
<th>Mode of Transportation</th>
<th>Technical Skills</th>
<th>Dedication (willingness to risk death or capture)</th>
<th>Inside Assistance</th>
<th>Planning</th>
<th>Ingenuity and Imagination</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-level composite</td>
<td>12-20</td>
<td>Anything up to and including light, crew-served weapons</td>
<td>High explosives, sea, power tools</td>
<td>Foot, commercial vehicles, air</td>
<td>High*</td>
<td>High*</td>
<td>Information and help</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

*High dedication and high skill are not generally seen in a single "typical" group, with the notable exception of many commando raids."
summarizes those attributes commonly seen, the high-level composite represents something near the upper bounds. The commando raids were not included in the high-level composite because they took place in a wartime environment, and we are concerned here with adversaries that plausibly might appear in a peacetime environment. It should be noted, however, that in most of the attributes, the high-level composite resembles the typical commando raid, except that commandos are unlikely to have inside assistance, an attribute we ascribe the high-level composite.

The high-level composite adversary is hypothesized to possess the following attributes:

- **A full range of motivations.** These range from monetary gain to the extortion of political concessions; they include blind anger and the desire to embarrass a corporation, an industry, or even the national government.

- **Between twelve and twenty perpetrators.** This represents a reasonable upper limit for the number on the adversary's personnel resources. More are possible but unlikely in the absence of serious civil disorder or war.

- **Inside assistance.** This could assume the following forms: information on facility layout, personnel, and security systems; diversionary actions; disabling of systems; assistance in the penetration of the security system and in its operations; and, of course, actual acts of sabotage.

- **Weapons and explosives.** Those observed in the database include pistols, shotguns, automatic weapons, grenades, devices constructed for specific destructive purposes, and light crew-served weapons. Adversaries have used a variety of explosives, including military, commercial, and homemade explosives. Weapons and explosives are available on the illicit market to any determined and well-funded adversary. What the adversary can carry and use during the actual operation, rather than what he can obtain, appears to be the main constraint on the amount of arms and explosives the adversary may bring to bear.
Tools and equipment for penetrating barriers and vaults. These include hand and power tools, sledgehammers, jackhammers, cutting torches, thermic rods (burn bars), saws, drills, some cordless power tools, and modern electronic equipment.

Sophisticated tactical communications equipment. Specific instruments observed included citizens band radios, military walkie-talkies, and field telephones.

Various modes of transportation. Cars, vans, trucks, helicopters, and a limited number of fixed-wing aircraft have been observed in incidents in the peacetime data base.

Adequate finances. Funds become a serious consideration when a group of adversaries must be maintained together over a period of time, but are unlikely to prove a critical restraint. The larger terrorist groups do not appear to have been unduly hampered by lack of funds. Possible means of financing violent acts are bank and other robberies, ransom payments, financial support from sympathetic parties, extortion, and personal funds.

A high degree of technical knowledge. Technical skills are varied and multiple, including weapons and tactics skills, breaking and entering capabilities, the knowledge and ability to falsify credentials, the ability to manufacture and use explosives, and a knowledge of smuggling techniques.

Experience. The high-level composite adversary can be expected to have previously conducted similar activities; he will not be a novice, especially as the difficulty of the operation increases.

High degree of imagination and ingenuity. In a large number of incidents, the adversaries were able to overcome imposing obstacles by mounting ingenious attacks and deceptions.

Willingness to risk capture or death. This was particularly apparent in the terrorist assaults and commando raids and conspicuously lacking in the symbolic bombings, sabotages, and capers.
-50-

- Ability to devote adequate time. In some cases, adversaries were able to dedicate a great amount of time to planning the action and securing the necessary resources. Very few cases were characterized by extemporaneous action.

- Rapid execution. Once under way, the adversary executed his plan with remarkable speed, in some cases in only a matter of minutes.

- Ability to maintain secrecy. This includes the ability to maintain intragroup discipline as well as conceal the group's plans from the authorities.

- Ability to achieve tactical surprise. This was a key to almost every successful incident, especially where security forces were lax because of the belief that their system was secure.

Implications of the High-Level Composite Profile

A combination of all the high-level attributes (see Table 4) in a single adversary is unlikely. The individual attributes or characteristics have been seen in the data base, but the concurrent appearance of all the characteristics has not been observed in any single adversary. Some of them actually appear to be mutually contradictory. For instance, the combination of a large, well-armed assault force, the capability to defeat modern alarm systems, and the ability to keep the operation completely secret are not attributes that normally occur together. The ability to neutralize alarm systems is used to penetrate a target without detection; in that case, a well-armed assault force would not be required. In fact, a large force would be counterproductive because it would raise the probability of premature detection. Conversely, if armed assault by a sizable force were planned, a technical capacity for alarm circumvention would not be necessary.

The highest degree of technical sophistication exhibited in any of the analogs has been observed in some of the burglaries, which involved circumventing electronic alarm systems and penetrating physical barriers. The burglars involved in these crimes were careful, cautious men, concerned with turning a profit without being captured. In most
cases, they were highly averse to taking risks. The burglaries, then, fall into the area in the lower right of the curve in Fig. 1. Similar observations may be drawn regarding the incidents of industrial sabotage, where the perpetrator is often likely to possess inside knowledge and specialized skills. In the terrorist assault, on the other hand, the situation is reversed. The perpetrators in terrorist assaults generally were more highly dedicated, sometimes to the point of suicidal fanaticism (such as that displayed in a few of the hostage incidents), and were often willing to risk death for their cause if called upon to do so. They were well trained as soldiers, not technicians, and the degree of technical skills they displayed was low. The terrorist assaults would generally fall at the upper left of Fig. 1. Any combination of these two attributes corresponds to some point on the curve; the greater degrees of technical skills fall further to the right of the origin, and a greater willingness to accept risk is higher

![Diagram](image)

**Fig. 1** — Likely combination of adversary attributes
above the horizontal axis. We can thus see that in practice this pair of attributes stands in opposition, i.e., one would not expect to find an adversary simultaneously exhibiting or possessing high levels of both.

We must caution the reader in the interpretation of this observation. It may well be that the hypothesized inverse relationship between technical sophistication and willingness to accept risk (Fig. 1) is not entirely a function of adversary capabilities. Rather, it may reflect the requirements of the task involved. For example, terrorists have shown little technical sophistication in their assaults because there was no perceived need; seizing an embassy or hotel lobby requires little technical skill. However, the terrorists in the incidents examined were, in many cases, members of larger groups with access to technical skills.

Contrary to most acts of terrorism, the capers examined that required a high degree of technical competence also required that the criminals avoid exposure; i.e., overriding dedication was not a typical attribute within this category. Burglars and armed robbers needed to escape with their loot to succeed, whereas terrorists were able to achieve part of their objectives if apprehended or even killed during their assault; indeed, their political aims required publicity, both for their cause and, occasionally, themselves.

Although it is not inconceivable that one might encounter adversaries in peacetime operations who are both technically skilled and willing to risk their lives, we have not found such optimal examples in the recent history of crime and political violence. Such a concentration of skills, motivations, and performance in an attack would represent a quantum jump from the previously displayed capabilities. It is conceivable, however, that if the objective appeared worthwhile to the potential adversary, he might be able to assemble a coalition that has clusters but not all the critical high-level composite attributes. These clusters might, for example, group great fire power, dedication, and planning, or technical sophistication, highly advanced tools, and ingenuity. Such clusters of attributes can be observed for a few adversaries in the data base. Again, the exception lies in commando
raids on well-defended industrial targets during war or similar periods of political stress.

In sum, the high-level composite represents an unlikely combination of high-level capabilities, with the exception of the commando raids, for three reasons. First, to date, adversaries have either lacked the necessity, the will, or the ability to assemble the materials, personnel, and skills that would make up the high-level composite. Second, some of the requisite attributes, if not contradictory, are at least incongruous in combination. Third, in the incidents reviewed, the necessity for assembling the high-level composite attributes was simply not present. The purpose of the high-level composite is not to depict a realistic nuclear adversary. As we have said before, it is merely a reference point. If the defense system can compel the adversary to possess the attributes of the high-level composite, it probably will have "priced most potential adversaries out of the market."
V. CONCLUDING OBSERVATIONS

While the analysis of the analog data base does not permit us to anticipate every type of adversary or every mode of threatening action, it does enable us to make a number of observations that are particularly relevant to the defense of nuclear facilities and to safeguarding nuclear programs. These include the critical attributes that a potential nuclear adversary might possess or be able to mobilize, their implications for security systems, and the dynamic nature of the threat.

CRITICAL ATTRIBUTES

In an effort to determine what limitations a potential adversary might possess, we have identified and examined the attributes and levels we judge to be especially critical if an adversary is to achieve success. By determining the requisite levels of these attributes needed, we can estimate the adversary's potential "breaking points," i.e., the points or levels at which the adversary seems to begin to encounter serious difficulties in assembling resources. Real-life adversaries have already demonstrated their ability to attain a high level in some attributes; in other attributes they face greater difficulties. This level or these breaking points are not determined by quantitative analysis. They are explicitly based on a reading of the current data and past Rand studies of criminal and political violence.

We first consider the number of persons who might participate in an actual theft or assault. The size of the force a potential adversary can deploy has received considerable attention from the security planners. It is a critical parameter in many engagement models used to establish the size of the guard force and other defensive requirements. One of the major lessons to be learned from the study of the analogs concerning the number of perpetrators is that, up to a certain limit, the size of the force employed by a determined adversary appears to be more a function of the requirements of the job than the adversary's capability to recruit. The fact that we have not seen many operations beyond the twenty-man level suggests that this may indeed
be a breaking point, although one cannot be entirely sure that greater numbers were not seen merely because the job did not require them. This predicament is inherent in the use of historical analogs as a basis of describing as yet nonexistent (or not yet active) adversaries. Still, the analog methodology affords greater reality and precision than mere speculation.

Theoretically, of course, it is possible that the adversary could assemble a hundred men to attack a nuclear site, just as it is theoretically possible that he could mobilize a hundred men to attack a bank. Moreover, since the type and motivations of persons or groups attacking nuclear targets might be different, the number of participants may also be different from those encountered to date in criminal pursuits. However, in realistic terms, there do seem to be some upper limits on the size of a potential adversary force. In today's world, the number of subnational groups able to mobilize large numbers of people for a single criminal operation is limited to a few major criminal organizations and to some of the larger terrorist groups based abroad.

Regardless of the strength and resources of a supporting group, there appear to be good reasons why most adversary groups in the 300 incidents we examined limited their numbers to less than eight participants. Recruiting capable and reliable specialists is a problem. Specialized training may reduce this problem, but it enlarges the scope of the operation even more. Security is a problem; the more people involved in the preparation, the greater the risk that somebody will reveal the operation and its members to the authorities or even that an informant from a security agency may be included. Operational problems increase (and chances of success diminish) with larger numbers; e.g., coordination, communication, command and control, transportation, and withdrawal problems become more diffused and difficult. Hence, the probability of a successful outcome of the operation becomes increasingly diminished as the number of participants grows. Moreover, the data base demonstrates that small groups of skilled people can be very effective. Large numbers are not necessarily needed. Single saboteurs and bombers have produced significant amounts of destruction and, in a few cases, small groups of commandos have succeeded where larger, more powerful
groups have failed. The implication is important: *Defense capabilities cannot be pegged to a predetermined number of postulated adversaries.*

Weapons and explosives are readily available in the United States and from abroad. Large numbers of automatic and even more destructive weapons (possibly remotely controlled weapons) have been stolen from military stocks and are available on the illicit market. Devices that may be used to debilitate the defense personnel, such as smoke and tear gas grenades, are similarly available. Explosives are obtainable commercially or by theft, and the information necessary to manufacture explosives from readily purchased materials is easily available. It must be assumed, therefore, that a determined adversary will have access to automatic weapons, munitions, and explosives if he requires them; in other words, he will acquire whatever he thinks he needs. The primary constraint on his arms and munitions capabilities will not be on what he can acquire but more likely on what he can carry and use.

Likewise, the availability of tools and equipment, such as power drills, cutting torches, and radios, should pose no problem to a well-organized, motivated adversary. Denying or restricting the availability of weapons or equipment is beyond the scope of the defense system. Hence, the system should be prepared to deal with a well-armed and well-equipped adversary.

The critical attributes determining the success of a venture seem to be the less tangible human factors: imagination and ingenuity; criminal and military skills; technical knowledge; the willingness to risk capture or death; inside assistance or privileged access; a capacity for maintaining group discipline and secrecy; the ability to achieve tactical surprise; and the necessary combination of several of them. These attributes are not susceptible to easy quantification and display on a chart. They are qualities that one talks about in terms of "they have it or they don't." Although it is more difficult to design defensive systems against them, it is not impossible. However, they require a different set of security requirements. Even if potential adversaries were accorded the numbers and resources seen in typical burglaries, robberies, sabotages, and assaults, their success or failure would largely depend on their possession or lack of ingenuity, technical
skills and knowledge, and the willingness to accept risk. It would be extremely difficult for any single potential adversary to possess high capabilities in all of these human quality attributes. Whether or not a successful assault on a nuclear facility for the purpose of theft or sabotage would be sufficiently attractive to cause a band of criminals or political extremists to surpass all levels of previously displayed talents and dedication depends very much on the nature and size of payoff they would anticipate and their own estimate of feasibility. This, however, involves the question of intention rather than capability, a topic that is the focus of companion Rand research in the context of nuclear safeguards.

POSSIBLE IMPLICATIONS FOR SECURITY SYSTEMS

It is not the intention of this report to specify the performance requirements or the design of security systems to protect nuclear programs and installations. However, analysis of the database does reveal certain strengths, strategies, and preferences on the part of the potential adversary that the designers of effective security systems should take into account, as well as certain vulnerabilities or aversions on the part of the adversary that might be exploited.

Armed robberies, terrorist assaults, and commando raids all show that an open, overt assault on defended facilities is likely to be avoided. In all cases, the perpetrators wanted to gain entry before confronting the defensive force. In most of these three types of incidents, there was no shootout with guards; more important, in those in which shots were exchanged, few were fired by the adversary attempting to fight his way in. When shooting did occur, it was often a diversionary tactic. It can therefore be assumed that by the time weapons are displayed by the adversary, his operation is likely to be well under way; i.e., insiders may have already done their part, alarms disabled, and the facility's defenses violated. Professional criminals and saboteurs are interested in avoiding armed combat altogether; even well-armed terrorists and commandos attempt to approach and penetrate a target without resorting to arms. It was often observed that once the initial defenses were compromised, a display of superior force by the
intruders and a neutralization of the initial defense response occurred. Again, an open, frontal assault on a facility's defenses generally seems to be an unlikely mode of approach and attack. An effective security system must therefore be alert to and guard against the nonviolent ways in which the system might be defeated.

In view of the fact that the mobilization of manpower up to a certain limit and the procurement of arms seem to pose little or no problem to the adversary, it appears that the defensive system should focus on exploiting the "human capabilities" (e.g., dedication and ingenuity) of the adversary. An adversary would have great difficulty assembling people who are technically knowledgeable, experienced in such skills as the operation of weapons, the use of explosives, the circumvention of alarms, the penetration of barriers, and dedicated to the point of risking their lives. A security system that compels a potential adversary to possess all of these critical human capabilities will deter or thwart a large portion of the actions that might be directed against nuclear programs.

In general, it appears from our data that physical barriers were sufficient in terms of delaying or hindering the adversary but not sufficient by themselves to defeat him. Thick walls of concrete and steel were breached if the operation went undetected. Penetration was more rapidly effected with the use of high explosives if the operation did not need to be covert, or quickly and quietly with the use of inside confederates. Incidents in the data base confirm that barriers, by themselves, do not appear to provide adequate security. They require special attention or monitoring if they are to be effective.

On the basis of our analysis, the prospect of physical danger did appear to have some deterrent value, especially if confronted while entering a facility. This was certainly true for professional criminals and even for some terrorists who seem to prefer undefended targets. Potential adversaries should be made aware that attempts to penetrate the sensitive areas of nuclear facilities will require them to risk their lives. Even then, there still may be small numbers of adversaries willing to go against armed defenses if the perceived rewards are high enough.
Terrorists have rarely assaulted facilities when a high probability existed that they might be defeated before they gained entry. But they were willing to assume great risks after they had gained entry and barricaded themselves (often with hostages). This suggests that standard containment or reinforcement strategies would be less effective against terrorists. A security system that would permit an adversary to carry out such barricade or barricade-and-hostage tactics would enable him to achieve his objectives by providing him with a highly visible public platform from which to publicize his political objectives and aims. To deter nuclear terrorists, it is essential that the defenses be structured to defeat a possible attack before the terrorists gain entry, rather than by trying to contain it after it is discovered.

Professional criminals have frequently tried, and have often been able, to recruit a person working inside the facility to provide them with some form of assistance, e.g., privileged information or access. Saboteurs often have internal assistance and information. Hence, the security system, indeed the entire facility, should take precautions to guard against the potential compromise of the installation by any single employee or member of the security force. Some measures have already been instituted, including rigid employee clearance procedures. The effectiveness of security clearances should be re-examined in this context. Because internal sabotage or assistance to a terrorist group poses a serious threat to the security systems of nuclear facilities, internal security measures regarding employees should be regularly evaluated and, if necessary, upgraded.

Because, in many instances, deception and diversion have been used successfully by adversaries—both criminal elements and political extremists—considerable emphasis should be placed on how to deal with these two common ploys in designing security systems and in formulating appropriate security and training procedures to defeat them.

Finally, the creation of uncertainty by the defender would appear to cause potential adversaries the greatest difficulties in planning and executing their acts. Uncertainty as a protective device could be enhanced by a security system designed to exploit it—e.g., by a security system having an armed and trained guard force whose immediate
strengths and routines could never be confidently predicted; or having multiple layers of defenses whose nature was shrouded in secrecy, perhaps reinforced by deliberate disinformation, or even decoy targets. In conjunction with strong, monitored physical barriers and a well-trained and well-equipped guard force, the use of uncertainty in planning a defense system would make it extremely difficult for a potential adversary to know what levels of attributes he would need. Faced with this uncertainty, he would be forced to assemble and employ effectively all the capabilities of the high-level composite—and he would still be uncertain of his probability of success, even based on a generous definition of what constitutes success. These requirements, then, should serve to defeat an adversary before he even poses a physical threat to the installations.

DYNAMIC NATURE OF THE THREAT

This analysis is based on prevailing political, economic, and social conditions in the United States and, of course, is subject to change if these conditions change. The United States is currently in a period of relative domestic tranquility, marked by occasional incidents of low-level terrorist violence that could conceivably become somewhat more serious in the future. With few exceptions thus far, foreign terrorist groups have not carried out operations in the United States. Domestic political extremist groups have not conducted extensive, violent activities against U.S. nuclear programs. Task force crimes do occur regularly in the United States, but there is no evidence indicating that professional criminals are attracted to nuclear materials or terrorism.

However, in the recent history of nuclear incidents, a faint escalatory trend may be discerned. More incidents appear to have occurred recently, although possibly this may simply be due to better reporting in the case of bomb threats and low-level incidents. It also may be due to the fact that there are now more nuclear facilities. Still, especially in light of the series of nuclear incidents in Europe
(1975-1977), these incidents do appear to be both increasing and more serious than anything previously reported.*

New political or economic conditions could alter the potential threat. For example, domestic political disorder might be accompanied by a proliferation of potential adversarial groups. Renewed American involvement in wars abroad might increase domestic dissent and the probability of sabotage against nuclear weapons assembly and storage sites. Even assuming no change in the current domestic political climate, it is possible that some individual or some group of criminals or political extremists could successfully carry out an action against nuclear targets here or abroad, thereby inspiring others and perhaps setting off a series of nuclear incidents similar to the airline hijackings that suddenly proliferated in the late 1960s. Moreover, nuclear plants are very newsworthy and, as such, fulfill the general high-visibility criterion important to many terrorist groups. It is not, therefore, farfetched to assume that they could be potential targets for terrorist activities and thus warrant careful protection. Yet, one should be cautious not to extrapolate from this observation and predict outright that nuclear facilities will be a terrorist target.

Lastly, the threat must be regarded as dynamic because we can expect that potential adversaries will continue to improve their technical skills, learn how to penetrate, overcome, or circumvent increasingly complex security systems, and acquire new weapons capabilities (for example, man-portable, precision-guided munitions) that may be useful for sabotage or theft operations. Similar improvements can be predicted in the defensive systems.

All the above factors suggest a continuing requirement for monitoring and reassessing the potential threat as it changes over time.

---

Appendix A

THREAT CHARACTERISTICS OUTLINE

1. WHO
   A. Political extremists
   B. Disgruntled employees
   C. Criminal elements
   D. Lunatics
   E. Antinuclear extremists
   F. Disgruntled public (anti-utility)
   G. Foreign agents (not included in our incidents)
   H. Mercenary

2. MOTIVES
   A. Economic gain
      1. Theft for sale or use
      2. Extortion (includes economic pressure)
   B. Anger (revenge)
   C. Political concessions (including publicity)
   D. Damage (symbolic) destruction
      1. Nuclear per se
      2. Nuclear incidental
   E. Other (e.g., irrational, insane, prankster)

3. ADVERSARY ATTRIBUTES
   A. Number of attackers
      1. One
      2. Two to five
      3. Six or more
      4. Unknown
   B. Armament
      1. None
      2. Commercial firearms
      3. Automatic weapons, grenades, explosives
4. Crew-served weapons
5. Armor, missiles
6. Clubs, etc.
7. Unknown

C. Knowledge
1. Publicly available
2. Criminal casing
3. Casual intelligence
4. Complete
5. Unknown

D. Operational training
1. None
2. Military
3. Criminal
4. Special military
5. Unknown

E. Equipment
1. Hand and portable power tools
2. Special tools and explosives
3. Heavy equipment
4. Unknown

F. Transportation
1. Cars and commercial trucks
2. Special vehicles
3. Aircraft
4. Unknown

G. Dedication
1. Sustained labor/discomfort
2. Injury/severe pain
3. Suicidal
4. Unknown

H. Technical training
1. None
2. Practical
3. Technical
4. Specialized
5. Unknown

I. Planning
   1. None or little
   2. Planning without rehearsal
   3. Planning with rehearsal
   4. Unknown

4. TACTICAL OBJECTIVES
   A. Within system
      1. Steal material
      2. Seize and hold facility/hostages
      3. Disable/disrupt facility/operations
      4. Hijacking
   B. Outside system
      1. Seize hostages—kidnapping
      2. Hoaxes/disinformation
      3. Inflict casualties

5. MODES OF ACTION
   A. Intelligence
      1. Public sources
      2. Inside knowledge
         a. Willing
         b. Unwilling
      3. Reconnaissance
      4. Unknown
   B. Access to facility
      1. Armed assault
      2. Barrier penetration
      3. Deception
      4. Inside assistance
      5. Disable alarm
      6. Legitimate access
      7. Barrier bypass, e.g., lock pick, window entry
C. Access to target
   1. Armed assault
   2. Barrier penetration
   3. Deception
   4. Inside assistance
   5. Disable alarm
   6. Legitimate access
   7. Barrier bypass, e.g., lock pick, window entry

D. Removal of material
   0. None or not applicable
   1. Diversion
   2. Theft
   3. Bookkeeping manipulation

E. Occupation and holding of target
   0. None or not applicable
   1. Hostages
   2. Gunpoint
   3. Barricade without hostages

F. Creation of damage
   0. None or not applicable
   1. Cause physical damage
   2. Misuse control mechanism

G. Neutralize people
   0. None or not applicable
   1. Yes

H. Egress
   1. Armed retreat
   2. Outrun system or response
   3. Stealth
   4. Bargain
   5. Deception

I. Publicize
   0. No
   1. Yes
6. **CONSEQUENCES**
   A. Success
   B. Partial success
   C. Failure

7. **CHARACTERISTICS OF THE OPERATION**
   A. Casualties (dead and/or wounded)
      0. No casualties
      1. 1-10
      2. 11-20
      3. 21-30
      4. Over 30
   B. Demands
      0. None
      1. Release of prisoners
      2. Safe conduct
      3. Release of publicity
      4. Other political
      5. Money
   C. Outcome
      1. Prisoners released
      2. Safe conduct granted
      3. Other political granted
      4. Surrender or capture of terrorists
      5. Assault by security forces
      6. Terrorists escape (not via hijacked aircraft)
   D. Duration
      1. Minutes
      2. 1-24 hours
      3. 1-3 days
      4. More than 3 days
   E. Time of Attack
      1. 8:00 a.m. to 5:00 p.m.
      2. After 5:00 p.m., before 10:00 p.m.
      3. After 10:00 p.m., before 8:00 a.m.
Appendix B

GLOSSARY

In this report, we have employed some terms the reader may not be familiar with, or we have used them to convey some very specific meanings. The following glossary has been compiled to facilitate the reader's understanding of certain words as they are used here.

Access: Methods or means employed by an adversary to enter a facility or to reach a target within a facility. Methods of access considered in the study include armed assault, legitimate access, barrier bypass or penetration, deception, inside assistance, and disabling of alarms. Multiple methods of access may be employed during a single incident.

Action: An illegal or violent action involving nuclear material or a nuclear installation, or an analogous type of action against some other type of target. Nuclear actions are of primary interest in the study, whereas analog actions are studied as a way of understanding the possible characteristics of future nuclear actions.

Adversary: A person or group of persons responsible for actions against nuclear facilities or involving nuclear material.

Aims: The longer-term or broader interests and objectives of the adversary, such as world revolution, elimination of nuclear weapons or nuclear power plants, or adherence to the word of God as he understands it from the voices in his head. The term is used in contrast to shorter-term tactical objectives associated with particular actions, such as gaining publicity for a cause or destroying a particular installation.

Analog action: A criminal or political act chosen for study because of its relevance to potential future nuclear actions.

Armed assault: A method of access involving the use of armed forces to subdue or overcome defenders. The term is taken to include cases in which weapons are employed only to threaten and subdue, but are not actually fired. This type of assault is frequently used in armed robberies, for example, and in some terrorist seizures of facilities, such as embassies.
Attributes: The physical characteristics, planning skills, and operational capabilities a potential adversary might possess.

Barrier by-pass: Circumvention or "end-running" of a physical protective barrier without actually engaging and defeating the barrier. Examples would be entry through an unsecured skylight or gate, or by climbing over the top of a fence or wall. The term is used in contrast to barrier penetration.

Barrier penetration: The defeat of a physical barrier by penetration of that barrier. Examples include tunneling, blowing open a safe or vault, cutting a fence, or breaking down a door. This term is used in contrast to barrier by-pass, in which the barrier is not directly engaged.

Capability: A quality not solely definable in terms of an adversary's equipment, numbers, or other material resources, or solely in terms of human capabilities (such as technical skills, dedication, or intelligence). It is a combination or sum of all of these.

Dedication: The intensity with which an adversary goes about his job and the risk and sacrifice he is willing to accept in its performance.

Egress: Getting out of a facility that has been penetrated and/or away from the immediate vicinity of the action. Methods of egress identified in the study include armed retreat, outrunning the response, stealth, deception, and bargaining. As with methods of access, one or more types of egress may be employed in combination in a single action.

Facility: A building or installation housing the target of interest to an adversary. In the burglary of a bank vault, for example, the bank itself is the facility and the vault within the bank is the target. In some cases, there is a clear distinction between facility and target, and access to one is no guarantee of access to the other. In other cases, the two may be essentially synonymous, at least from the point of view of access. This is true, for example, when the objective of the action is to seize and hold a facility, such as an embassy.

Hostage: Someone held by the adversary against his will, usually as a bargaining chip of some kind. Hostages are often taken in seizures
of a facility to deter a counterassault action by the facility's security system to retake the facility and to aid in bargaining for safe release. Hostages may also be kidnapped and held in unknown locations, sometimes as a means of coercing insider assistance.

**Inside assistance:** Persons who assist the assailants with information, force, or in other ways. Any attack by stealth or force, designed to accomplish any of a range of adversary aims, may involve inside help. These inside helpers may be voluntary accomplices who have infiltrated the installation ab initio for the purpose of the crime, or they may be employees who were subsequently recruited. Assailants may also obtain inside assistance by coercion, either directly, perhaps by means of threats against the individual himself, or indirectly, as by holding a family member.

**Inside job:** The inside job is distinguished from inside assistance in that it is planned and carried out primarily by insiders.

**Intent:** Purpose of the adversary activity. It encompasses both the immediate tactical objectives, such as theft of special nuclear materials or destruction of a facility, and the aims, such as obtaining publicity or money, mobilizing public opinion against the nuclear industry, discrediting the government, or attaining other goals.

**Motivation:** Differs from intent in that it describes the psychological mainsprings of the adversary activity. This may take the form of frustration, anger, a search for grandiosity, or political or anti-nuclear beliefs, or a number of other psychological factors. It is used to describe intrapsychic phenomena.

**Nuclear action:** An illegal generally violent action involving nuclear weapons or a nuclear installation.

**Objectives:** The specific tactical purpose of an action designed to serve the longer-range aims of the adversary. For example, the destruction of a nuclear power installation would be an objective; the aim would be to discredit the nuclear program or possibly to force political change.

**Professional criminal:** A person who makes his living primarily through criminal activity. In the process, he may have "professionalized" certain skills needed to carry out his crimes. He may or may not be a member of organized crime.
Symbolic attack: Deliberate acts of destruction or violence, often bombing, calculated to express a grievance or to make a political statement. The target is perceived by the adversary as having symbolic significance; the damage to the target may be secondary or even irrelevant to the adversary's aims.

Target: The thing the adversary is after—money or valuable material in a robbery or burglary; the object he wants to destroy in a bombing or other destructive act; a weapon; etc. For some types of actions, the target and the facility involved may be the same, and no distinction between the two is necessary. This is true, for example, when seizure of a facility is the objective of the action. For other types of actions, such as burglary, the distinction between the target and the facility that contains it is a natural and useful one.
Appendix C
ADVERSARY ATTRIBUTES

NUMBERS
  o Number of people independent of other factors

EQUIPMENT
  o Hand tools
  o Power tools
  o Explosives
  o Heavy equipment
  o Specialized

ARMS
  o Small arms
  o Explosives
  o Automatic weapons
  o Tanks

TRANSPORT
  o Foot
  o Car or truck
  o Aircraft
  o Special

KNOWLEDGE
  o Casual
  o Public research
  o Criminal
  o Intelligence and insider

DEDICATION
  o Casual
  o Discomfort
- Injuries
- Loss of life

**TRAINING**
- Planning level
- Degree of training
- Tactics