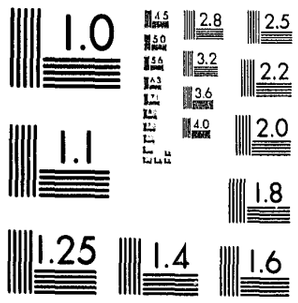

ATTRIBUTES OF POTENTIAL ADVERSARIES TO U.S. NUCLEAR PROGRAMS[1]

Allan M. Fine

Sandia Laboratories, Albuquerque, NM 87115

INTRODUCTION

Sandia Laboratories, in its activities as a prime contractor for ERDA, has been heavily involved in the research and development of physical protection elements and systems applicable to the protection of nuclear facilities and materials. A part of this effort has involved the characterization of potential threats to U.S. nuclear programs. The Rand Corporation, under contract to Sandia Laboratories, has investigated several hundred incidents which involved activities that could serve as analogs of potential threats to U.S. nuclear programs. This paper summarizes the data used by Rand and provides a listing of potential adversary attributes derived from a historical-incident data base. The attributes are expressed in terms of the capabilities of a composite adversary group.

DATA BASE INFORMATION

In the United States, no nuclear installation has been attacked, seized, or effectively sabotaged; no nuclear weapons have been diverted or illegally detonated; no nuclear materials have been stolen or taken by force or used for blackmail or made into an explosive device; and no radioactive materials have been maliciously released. Although there have been telephoned bomb threats to many U.S. commercial and governmental nuclear installations, some minor industrial sabotage related to labor problems, and some accidents resulting from poor training or inferior procedures, no major incidents concerning U.S. nuclear programs have occurred.

Outside the United States, more serious events involving nuclear materials and facilities have occurred: political extremists have sabotaged reactors in France; urban guerillas have seized control of a nuclear power plant in Argentina; and a mentally disturbed individual has spread radioactive materials on a train in Europe. While these events are serious, they have not occurred in sufficient numbers to permit extrapolation to adversary attribute characterization for use in describing potential threats to U.S. programs. However, inclusion of these types of incidents in a more general data base of information can yield insights into the *modi operandi* of perpetrators of such actions and provide utility in characterizing U.S. program needs.

While it is fortunate that no major incidents involving U.S. programs have occurred, conversely security analysts have little hard information on the basis of which to postulate potential adversary characteristics. Because of this factor, it has been necessary to go outside the nuclear program realm and to examine incidents which could provide data on potential adversaries in terms of analogous events which have characteristics transferable to potential nuclear incident perpetrators. Rand analysts have used this approach to provide a set of analog incidents—historically based, factual, and detailed—to accumulate a data base. This data base is intentionally limited in scope and is capable of providing information from the incidents chosen for a relatively

[1]This work supported by the U.S. Energy Research and Development Administration.

select group of questions relating to perpetrator attributes observed or determined from the action incident. The attribute list for which the data base incidents have been chosen includes:

- Number of attackers
- Armament
- Knowledge (technical, operational)
- Training (technical, operational)
- Equipment used
- Transportation modes
- Dedication to mission
- Planning for mission
- Overall resources available

The various types of events used as analogs are:

- Sophisticated crimes: Robberies and burglaries by groups against high-value, protected targets for monetary gain.
- Symbolic bombings: Bombings by groups of political dissidents for material damage.
- Terrorist attacks: Seizures of facilities and/or hostages; group action for political gain.
- Sabotage: Actions by individuals or groups to damage facilities.
- Large scale extortion/hostages: Group actions for massive political or economic gain by threat of wide-scale damage.
- Mass casualties: Historical use of weapons or acts to kill large numbers of people for political gain.

  Wartime incidents of dedicated groups attacking defended targets.

SPECIFIC ANALOG PROFILES

Rand analysts have completed work on several analogous incident reports and have others in process. In order to provide a listing of attributes, several analogous incidents were selected for concentrated study. The data base for these contains nearly 200 incidents covering sophisticated crimes, terrorist assaults, and bombings. These events were selected because their characteristics approximate the intentions and capabilities believed to be required for attacking or penetrating a nuclear facility by stealth or force of arms for the purpose of seizing hostages, sabotage, or theft. For each of these analogous incident types, a profile of typically displayed attributes has been compiled and a general profile of the typical attributes—based on a combination of the specific profiles—has been derived.

PROFILE 1. TASK FORCE CRIMES OR "CAPERS" (ROBBERIES AND BURGLARIES)

The data base in this category comprises crimes committed by groups of people, some of whom are highly specialized and skillful. The perpetrators assemble for the specific operation and form "task forces" organized for assaults on well-protected objectives such as bank vaults and museums. The prizes sought are substantial, and the adversaries display some high-level capabilities. Specialists involved may include but not be limited to safecrackers, electronics experts and communications experts. The current data base of nearly 200 incidents includes 46 such crimes. Of these, about three-fourths were committed in the United States and one-fourth abroad, primarily in Canada. Most are burglaries (involving surreptitious, forced, or illegal entry); the remainder are armed robberies, such as the famous Brinks robbery in Boston, or attempts to release prisoners. One of the prison breaks and an arsenal robbery involved members of political extremist groups; none of the other task force crimes had political overtones.

Almost all of the cases examined were successful. The adversaries evaded or overcame the security measures and escaped with the goods. It would be instructive to examine failures as well

as successes, but information on these is hard to obtain. The professional criminals involved appear unwilling to assume major risks; confronted with high risks of failure or apprehension, they are likely to abort the operation. Of course, failures generally are not as well publicized as spectacular successes, making it difficult to even know about them; unless the perpetrators are apprehended, there are few means of determining what resources they had assembled for their attempt. Figure 1 is a listing of the task force crimes profile.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
				"ROBBERY"				
3-6	Handguns, shotguns	Hand and power tools	Foot, commercial vehicles	Mid	Mid	Information	Mid	Mid to high
				"BURGLARY"				
2-4	Usually not displayed	Explosives, and power tools	Foot, commercial vehicles	High	Mid	Information	High	Mid to high

FIGURE 1. *Task force crimes profile.*

PROFILE 2. ASSAULTS

This portion of the data base includes 32 terrorist assaults. Of these, 23 were related to the conflict in the Middle East: eight took place in Israel, four elsewhere in the Middle East, seven in Europe, three in Asia, and one in Latin America. The targets of 14 of these incidents were Israeli assets, including El Al offices, aircraft, diplomatic posts, and personnel outside Israel. Arab assets (e.g., embassies) were the targets of two incidents; U.S. assets or citizens were the targets of six incidents, including an 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 assaults took place in Latin America and six took place elsewhere: the seizure of a train and of the French embassy in the Hague and the seizure of the U.S. embassy in Kuala Lumpur, an assault on the German embassy in Stockholm, and an attack on a San Francisco police station. Although the risks involved in the terrorist assaults exceed those involved in the task force crimes, for the most part these were assaults on soft targets; the assailants could expect at least to seize control of the facility or hostages without running into serious armed resistance. Figure 2 is the profile of attributes of the "typical" terrorist assault.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
3-6	Handguns, automatic weapons	High explosives	Foot, commercial vehicles, air	Mid	High	No	High	Mid to high

FIGURE 2. *Typical terrorist assault profile.*

PROFILE 3. BOMBINGS

The current data base consists of 108 bombings which occurred between 1965 and 1976 in the United States. The targets were about evenly divided between commercial facilities (e.g., corporate headquarters and banks) and government facilities (e.g., office buildings and consulates). However, a few residences were involved. The bombings were mainly of soft targets; attacking them presented little risk to the perpetrators. Most had minimal or no security system. The bombers were motivated by political extremism, personal animosity, anger at particular corporations, and anger at or resentment of public officials or the acts of public agencies. The total casualties of the bombings were four dead and 69 injured. Figure 3 is the typical bombing profile.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
1-2	Explosives	Hand tools	Foot, commercial vehicles	Mid	Low	No	Mid	Mid to high

FIGURE 3. *Typical bombing profile.*

PROFILE 4. COMPOSITE FOR U.S. ACTIONS

By combining the attributes of the analogous incidents shown, a composite model, figure 4, of attributes has been developed. The composite is based on typical values from each of the contributing profiles. An adversary group adhering to this composite might exhibit the following characteristics: three to six perpetrators armed with hand guns, shotguns, and automatic weapons; access to and egress from a target by almost any type of commercial land vehicle; tools used could be hand-held, portable power tools, and there could be limited use of high explosives. The group would have the benefit of good planning for the mission and would exhibit sufficient ingenuity, technical and operational skills to provide for proper execution of the operation. Group members would be sufficiently dedicated to the group and its mission to risk capture or injury. Assistance or information from an insider could help the group complete its mission.

It is important that the composite profile not be misconstrued or misrepresented. It represents the typical profile of potential adversaries as derived from other profiles of selected incidents believed to be analogous and transferable to potential adversary activities relating to U.S. nuclear programs. The composite is *not* a description of "the threat to U.S. nuclear programs," nor is it intended to describe "the current threat" to any facility. It is a description of typical values of

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
3-6	Automatic weapons, grenades, shotguns	Hand tools, power tools	Foot, commercial vehicles	Mid to high[1]	Mid to high[1]	Information or other assistance from one "insider"	High	Mid to high

[1]Generally not seen together at high levels.

FIGURE 4. *Composite for U.S. actions.*

characteristics of adversaries observed in the perpetration of malevolent actions. The insights gained in the description of these characteristics are intended to provide a basis for consideration of adversary threat characteristics to any security system.

There is nothing in the "typical" profile to preclude individual attributes from taking different values from those listed; in fact, the episodes used for data base information in formulating profiles contain items in which many of the attributes of the typical profile are exceeded. An interesting tabulation can be constructed by combining the high levels of attributes found in the various analog incidents and making a "high level" analog composite. Such a tabulation is an artificially constructed one because the higher level attributes represent values not seen in the basic data as combined high-level attributes, but rather as an individual high value within a given analog incident.

A high-level composite profile based upon high levels of attributes from the analog incidents is shown in figure 5. For this high-level composite, the number of perpetrators is increased to a range of 12-20, armament is enhanced to include crew-served weapons, transportation includes aircraft, and other related attributes are all at the high level.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
12-20	Anything up to and including crew-served weapons	Explosives, power tools	Foot, commercial vehicles, air	High	High	Information and possible active help	High	High

FIGURE 5. *High-level composite profile.*

Analysis of the data base incidents by Rand analysts indicated that many of the attributes listed at the high level do not generally appear at a high level within sets of analog types of incidents. As an example, figure 6 shows a generalized plot of two of the attribute characteristics—dedication and technical sophistication. At the high level of dedication (risk of capture, injury, or death), one finds many perpetrators of terrorist assaults; at the high level of technical sophistication appear perpetrators of sophisticated burglaries. These characteristics are found as extremes in two different types of activities, while in the high-level composite profile (fig. 5) they appear together (upper-right region of fig. 6). The high-level composite calls for the combination within a group of diverse characteristics which leads to the conclusion that such a combination is of low likelihood and thus contributes to the artificiality of the high-level composite profile as a derivative of the analog data.

There is no reason to believe that a group of adversaries could not contain large numbers of people, could not use aircraft or helicopters, could not have crew-served weapons, and could not possess all the high levels of attributes in areas of skills, planning, and dedication. There is no justification to believe that such an adversary group could not exist; however the data from historically-based perpetrator incidents have not indicated that such a group has existed outside of wartime, nationally-sponsored, military experiences. For the non-war, sub-national, potential U.S.-based adversary, a group possessing all the attributes of the composite high-level profile would be expected to be extremely rare.

Analysis of the analog incidents, profiles, and composites has led to the tentative conclusion that physical attributes do not appear to be the most critical for an adversary. The high-level composite was constructed to show some degree of criticality in attributes for a potential adversary, that is, those attributes which appear critical to an adversary to assure the success of a mission. It

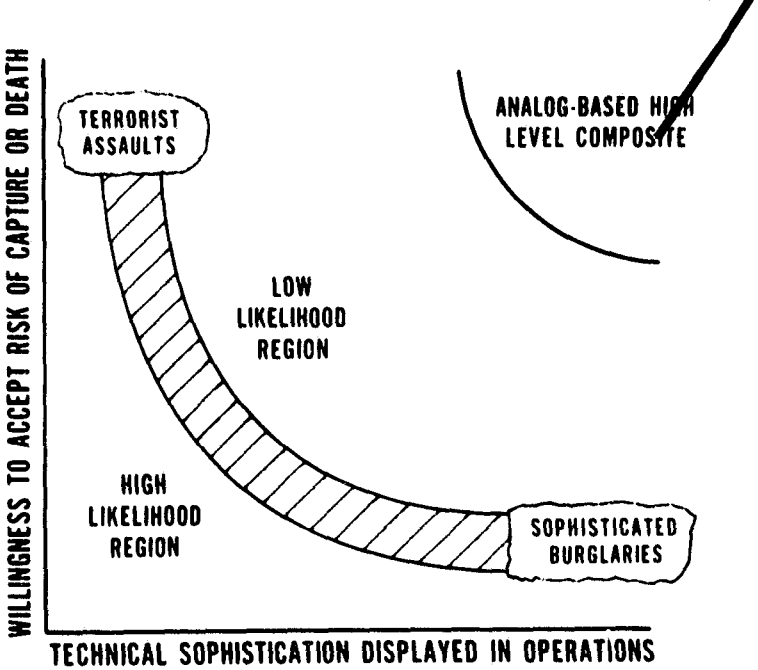

FIGURE 6. *Dedication vs. sophistication.*

appears that human factor type attributes, in combination, may be the most critical ones for a potential adversary group to possess. In the United States today, it is not difficult to obtain arms, ammunition, explosives, tools, equipment or specially skilled people for a specific task. Given that these physical attributes are available, other factors appear as critical constraints to potential adversaries. The critical factors which quite often decide the success or failure of a mission include:

- Imagination and ingenuity
- Criminal and military skills
- Technical knowledge and capability
- Dedication (willingness to risk capture, injury, or death)
- Fostering or cultivating inside assistance for a mission target

SECURITY SYSTEM IMPLICATIONS

The use of analog incidents and attribute profiles provides a means to generalize the needs of generic security systems in terms of defending against an adversary group possessing the given characteristics. Two aspects of physical security arise in consideration of the attribute listings: physical attribute defeat and human factor deterrence.

A security system should extract some minimum "price of entry" from an adversary in terms of requiring the adversary to possess the high levels of physical attributes. The more a security system tends to force a potential adversary toward the difficult-to-obtain high-level composite attribute list, the more severe will be the requirements for the adversary to assure a successful mission. Barriers, fences, alarms, guard forces, surveillance, and vaults are among the security related items which can contribute toward forcing an adversary to high, possibly detectable, levels of resources.

In terms of thwarting the critical attributes of a potential adversary, a security system should pose danger and risk to adversaries; it should possess features which are "mysterious" or unknown to outside (and many inside) personnel; it should promote change in appearance, tactics, and routines just for the sake of change; and it should utilize updated equipment to the degree necessary and commensurate with the material or facility to be protected. The combination of elements useful in thwarting potential adversary capabilities may vary from facility to facility, but the general theme is to create conditions which attack those attributes of skill, knowledge, dedication, and planning capability, and either deter the adversary group directly or force the group to go to extremes to provide the resources for a mission.

FUTURE WORK AREAS

The adversary attribute study by the Rand Corporation is continuing. Attribute description and data base information are in preparation and will be updated throughout the year.

In addition, the program has started to include an investigation of individuals and groups in relation to the motivation and intent of perpetrators of malevolent actions. Coupled with this will be a study of target attractiveness and operational planning factors relating to the individuals and groups studied. A report covering the combined physical and motivational attributes of potential adversaries to security programs will be provided as the terminus of the currently funded program. Future work is expected to include the updating and expansion of the data base for all attribute types contributing to potential threat characterization.

END