GENERIC ADVERSARY CHARACTERISTICS AND THE POTENTIAL THREAT TO LICENSED NUCLEAR ACTIVITIES FROM INSIDERS

Sarah Mullen

Division of Safeguards
U. S. Nuclear Regulatory Commission

GENERIC ADVERSARY CHARACTERISTICS AND THE POTENTIAL THREAT TO LICENSED NUCLEAR ACTIVITIES FROM INSIDERS

Sarah Mullen
Division of Safeguards
U.S. Nuclear Regulatory Commission

NRC has been charged by Congress with the responsibility for provision and maintenance of safeguards against theft and sabotage of licensed nuclear materials and facilities. In the discharge of this mandate, the Commission directed the Division of Safeguards to undertake two studies: one aimed at a systematic determination of the characteristics of potential adversaries to nuclear programs and the second aimed at a more detailed examination of the potential insider adversary.

The first study, entitled Generic Adversary Characteristics (GAC), was intended as an initial NRC effort at threat definition. It entails an analysis of characteristics associated with subnational conventional crimes and terrorist actions that could be analogous to potential nuclear events. Notce I said "analogous"--since adversary actions directed against nuclear facilities have been so few, we relied on an analog methodology under the assumption that a study of serious non-nuclear crimes can provide insights into the characteristics of potential nuclear adversaries.

p102

The data sources for the study consisted of over 650 articles, studies, books, NRC reports and memoranda, as well as interviews with Federal experts, criminologists, psychiatrists and social scientists.

The study addressed six generic adversary groups: terrorists, organized/sophisticated criminals, extremist protestors, disoriented persons, disgruntled employees, and miscellaneous criminals. They constituted the perceived range of possible threats of concern to us at the time. Data were drawn from incidents wherein laws were broken or in which criminal intent was obvious. We integrated the results of the data analysis into an adversary characteristic matrix like the one you received. Each column of the matrix represents a composite profile of one of the six generic adversary types based on observed actions and behavior.

Please recognize that these composites do not represent the upper or lower limits of adversary characteristics. Rather, they are the characteristics commonly found in the criminal acts we reviewed. As such, they can be considered representative of the characteristics that might be exhibited by such groups should they target nuclear activities in the near future.

I don't have the time today to discuss the matrix in detail, but I would like to mention briefly some of the study's conclusions. First, one of the least likely methods of attack is an overt armed assault. Even highly dedicated terrorists usually choose to approach their targets without resorting to arms, preferring to display firepower only once inside and in control of a facility. Second, physical danger appears to have some deterrent effect on all adversaries except the psychotic. Most adversaries proved to be risk avoiders. Third, organized and professional criminals often recruit insiders to provide them with some form of assistance, and disoriented persons, disgruntled employees, and white-collar criminals usually operate as insiders.

Finally, pegging defense capabilities to some predetermined number of postulated adversaries might be an inappropriate tack for security planners since behavioral characteristics such as motivation and dedication appear to influence adversary success at least as much as group size.

The Insider Study addresses the two types of insider crime that are the primary concern of nuclear safeguards--theft and sabotage--and focuses on the insider adversary, one whose authorized access to a facility or activity may be exploited by him or others in the commission of a crime.

The three objectives of the study are shown here. Data used in fulfilling these objectives were derived primarily from case histories of insider crime, but also from expert opinion and from non-NRC studies. Today, I will concentrate on objectives one, two and the prevention portion of three.

As with the GAC, we relied on an analog approach. Our criterion for determining which of the cases we gathered were the best analogs was the degree to which the safeguards systems in place at the time of the crime approximate the safeguards required of nuclear licensees.

From the cases that met our criteria, we extracted data on a variety of characteristics of the insider adversary and grouped them into the four categories shown on this vu-graph: position-related (e.g., screening and length of service); behavioral (such as motivation); resource (e.g., group size and equipment); and operational (such as tactics).

The major sources of data for the study fall into the two categories shown--U.S. Government agencies and private industry. Examples in the first category include the FBI, Department of Energy, and Bureau of Engraving and Printing. The second category includes money handlers, such as banks and casinos; material handlers, such as drug firms and chemical manufacurers; and money or material transporters, such as explosives carriers and armored transport companies.

In presenting the results of our characteristics analysis, I will be addressing the typical insider thief, the typical insider saboteur and a comparison between the lone thief and the theft conspiracy. First, the thief. The typical insider thief acted alone in 70% of the theft cases, whereas 10% involved two insiders and 20% three or more insiders. Typically, and not surprisingly, the insider thief was motivated by greed, indebtedness or financial inducement. These money-related motivations accounted for 74% of all the motivations identified. The next most frequently occurring motivations were drug use/abuse (6%) and personal loyalty (5%). The largest percentage of insider thefts (38%) occurred during the 6-10 year period of employment, 27% in the 3-5 year time period, and 19% during the first two years of employment. Approximately 80% of the insider thieves planned their crimes well or moderately well. By the way, all of these figures are based on 112 cases of insider theft involving 237 insiders.

Next we looked at the role of the insider, defining role as either overt or covert. By "overt" we mean that the insider was able to perpetrate the crime in the presence of others without arousing suspicion. "Covert" means that the insider was unable to carry out the crime in the presence of others without arousing suspicion. Approximately two-thirds of the insider thieves relied on covert activity to commit their crimes. Lastly, in 87% of the cases, equipment necessary to commit the crime was available at the site of the theft. Although not shown on the vu-graph, we also gathered data on the insiders' level of pre-employment screening. Over 40% of the insider thieves had received poor screening or none at all, with only 11% receiving high-level screening and just a handful undergoing psychological evaluation.

Before looking at the typical insider saboteur, I would like to emphasize that our sabotage analysis is based on a small data base, and thus our findings represent a limited characterization. First, 85% of the analogous sabotage cases were committed by a single insider. Although no one motivation dominated the insider saboteur, the combined motivations of psychological problems, disgruntlement and revenge accounted for 54% of the identified motivations. Approximately two-thirds of insider saboteurs committed their crimes in the first two years of employment, and they tended to plan less well for their crimes than did the thieves. In fact, about one-third of their actions could be characterized as spur of the moment acts executed against targets of opportunity. The insider saboteur, like the thief, relied on covert action 88% of the time and most frequently used equipment that was readily available at the site of the crime. As with the thief, psychologcal evaluations were rarely administered and over a third had received poor screening or none at all.

The next three vu-graphs depict a comparison between the single thief and thieves who operate in conspiracy.

For nearly every case in the data base, we identified the one or more generic weaknesses in the security system that rendered it vulnerable to the insider adversary. The five vulnerabilities shown here are the ones that most frequently accounted for the success of the crimes we analyzed and were most often cited by government and industry experts. Let me say a few words about the fourth entry. Personnel security deficiencies include inadequate pre-employment screening, insufficient behavioral observation, and poor management/employee relations. These three deficiencies contributed to the success of about 15% of the theft cases and about 70% of the sabotage cases.

Inadequate screening was judged a vulnerability when it was discovered after the fact that the insider had a criminal record that made him a poor risk or that he had a history of emotional instability that cast doubt on his ability to function reliably. Insufficient behavioral observation was applied when the malevolent insider suffered from a psychological or personal problem (including drug abuse) that should have warned an alert co-worker or supervisor to potential difficulty. Poor management/employee relations refers to situations in which management failed to provide a mechanism for airing and resolving employee grievances or proper recognition and incentives for its employees.

In assessing prevention method effectiveness, we looked at a number of different techniques now in use in industry and government and derived some implications about the prevention strategies shown. For today's symposium, I will discuss only the first three methods listed.

As for screening, our data suggest that it is an effective theft control strategy, and most of the experts we interviewed strongly advocated its use. Its effectivesness arises from several factors. First, it's generally accepted that a potential adversary may be deterred from even applying for a job at a facility that employs screening. Second, it conveys to prospective employees, as well as to those who are eventually hired, that the organization is concerned with insuring a high degree of integrity among its workforce. And third, good screening correlates with reduced conspiracy formation. Of a l the insider thieves in our data base who underwent "good" screening (i.e., screening based on a full-field background investigation or its equivalent), about 60% acted alone with 40% acting in conspiracy with other insiders. This table also suggests that screening must be "good" to make a difference because for any level of screening less than "good," the results are nearly the same: more conspiracy formation. (The total number of insiders represented by this table is 169.)

With respect to government clearances, we found the following. A clearance cannot be expected to provide full assurance of future trustworthiness because any number of factors can impair employee stability and reliability after hire. It can, however, reduce the likelihood of infiltration by criminal or terrorist elements and lessen the chances that a facility will hire persons who misrepresent their identities or backgrounds or persons with histories of relevant criminality or emotional instability.

Behavioral observation appears to pick up where screening leaves off by providing a post-employment means of recognizing and dealing with instability or aberrant behavior in employees. By so doing, behavioral observation can increase employee reliability after hire, but for such a program to be effective, three elements are necessary. First, employees' baseline stable behavior should be identified at the time of hire. Second, supervisory personnel must be properly trained to recognize aberrant behavior. And third, criteria for determining unreliability must be unambiguous and applied equitably.

Less data was available to us on the subject of psychological evaluations because many of the industries we contacted do not employ this technique due to privacy act considerations. However, the technique is widely used in police departments and the intelligence community. Generally, we concluded that psychological assessments can be an effective adjunct to screening and behavioral observation if they are evaluated by professionals, but that great care must be taken to prevent their misuse and mitigate their intimidating impact on personnel. Psychological evaluations may be especially important in preventing sabotage, which was often motivated by psychological problems.

Since the Insider Study was completed last summer, the Commission has taken action with respect to the pre-employment screening issue. In November, NRC issued a final rule requiring individuals who have access to or control over strategic quantities of special nuclear material to be cleared for such access through an NRC-administered personnel security program. Affected individuals will undergo government background investigations concomitant with their level of access at the expense of the licensee.

More recently, the NRC Staff is preparing for Commission review a rule that will govern access to non-weapons-grade nuclear material at power reactors. This program would be administered by reactor licensees themselves, not by NRC. As currently envisioned, and I emphasize that this rule is still in the draft stage, the program will consist of three components. First, a background investigation, perhaps with FBI criminal record checks initiated by the licensees. Second, psychological assessment, consisting of two written personality tests, one geared toward "abnormal" behavior patterns and one toward the "normal" adult population, and a clinical interview for individuals whose test results are questionable or indicate abnormal personality traits. And third, a post-employment behavioral observation program to detect psychological changes that may be manifested as behavioral changes in job performance, competence or judgment capabilities. As for the psychological tests, the NRC has determined the MMPI and the 16PF to be acceptable instruments for use in this program. Should a licensee wish to use other inventories, he would have to establish that they meet a number of standards, including high test-retest reliability and statistically validated scores. Both the tests and the interview should be based on the criteria shown here, which are measures of behavioral unreliability that have been shown to be relevant to the nuclear work setting.

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
ORGANIZATIONAL CHARACTERISTICS						
1. Organization	Well organized, hierarchical, bureaucratic, specialization common, compartmentalization practiced.	Efficient, hierarchical, bureaucratic (TOC)* No specific organization (WCC & CC)**	"Range" of organizational structure from no formal organization to well organized groups (i.e., collectives, small cells, etc.).	Little or no formal organization except for the psychotic cult. Anti-socials may belong to some organized criminal entity	Little or no formal organization with the exception of organized strike violence	Little or no formal organization
2. Recruitment	Universities, prisons, vocational training centers, refugee camps and ethnic population centers	Self-corrupted Blackmail Criminal Birthright (TOC)	High schools, universities, prisons.	Psychotics and neurotics exhibit no propensity to recruit others - they operate alone. Anti-socials often recruit others for criminal acts.	Normally operate alone and do not recruit others. Recruitment may occur within labor groups during organized strike violence.	Often act alone If others are recruited, they normally are associated with street criminal "clan."
3. Financing	Criminal activities robbery, kidnapping/extortion Donations by foreign countries, intelligence agencies, other terrorist groups, private citizens.	Criminal activities, gambling, drug sales, loan sharking (TOC) Legitimate business investments (TOC) No sustained financing other than personal resources (WCC/CC)	Criminal activities: robbery, fraud Legitimate jobs, parental assistance, donations	Use of personal funds as necessary. Normally, no financing required. Drug addicted commit crimes to finance habit	Use of personal funds as necessary. No significant degree of financing required	Criminal activities as appropriate No significant degree of financing required
4. International Connections	"Very High" - training, political support and financing from many Third World and Communist states Extensive contacts between groups	"High" - Worldwide (TOC) "Very Low" - None determined (WCC & CC)	"High" for Western European groups. "Low" for domestic groups.	"Very Low" - none determined.	"Very Low" - none determined	"Very Low" - none determined

A Examples include Baader-Meinhof Gang, Red Army Faction, PLO, Red Brigades, IRA, SLA, FALN, Anti-Castro Cubans, etc.

B Examples include (a) traditional "family" oriented groups (e.g., Mafia in Chicago); (b) ethnic "family" oriented groups (c) matrix oriented groups; (d) one-time operating groups (e.g., Brinks and Pendleton robberies); (e) computer crimes; (f) other sophisticated crimes/capers.

C Politically motivated, issue oriented acts of violence or criminality -- normally of symbolic nature. Differentiated from terrorist acts in that violence is generally low level. Terror is not an objective.

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc.

E This group also includes former employees.

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime

SCALE:

Very Low — Low — Moderate — High — Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
OPERATIONAL CHARACTERISTICS						
5. Planning	"High" - Normally involves target intelligence gathering, casing, and careful preparation.	"Very High" - Detailed preparation to include casing and rehearsal	"Unknown" - Planning detail not known for most domestic groups. Western European extremists exhibited careful planning.	"Range" of planning. Acts often spontaneous and involve no planning, other times detailed preparation	"Low" - little evidence of extensive or long term planning	"Very Low" - little or no planning
6. Timing	Function of political, symbolic and operational objectives and requirements	Timed to minimize risk of discovery - most "operationally" expedient moment.	Function of political, symbolic and operational objectives and requirements.	"Contagion" timing effect for psychotics. No other discernible timing pattern - individual unique.	Most acts timed to minimize risk of discovery - most "operationally" expedient moment	Often spontaneous and unpredictable Maximize "operational" chances of success
7. Tactics	Bombing most common. Also, assassination, armed attacks, kidnapping, skyjacking	Deception, diversion and crimes such as theft, fraud extortion, hijacking, corruption, bombing	Bombing most common. Violent demonstrations, property destruction, sabotage	Bombing, arson, skyjacking, hostage taking, multiple homicide, sabotage, fraud	Bombing, sabotage, theft, intrusion, property destruction, vandalism	Burglary, theft, assault, drug sales, forgery, bombing
8. Collusion (Insider)	"Very Low"	"High" - insider assistance frequently sought (TOC) "Very High" - most often are insiders (WCC & CC)	"Very Low"	"Moderate" - individuals may in fact be insiders.	"Very High" - most often are insiders	"Low" - however, inside information is frequently sought as opposed to using individual inside

A Examples include Baader-Meinhof Gang, Red Army Faction, PLO, Red Brigades, IRA, SLA, FALN, Anti-Castro Cubans, etc.

B Examples include (a) traditional "family" oriented groups (e.g., Mafia in Chicago); (b) ethnic "family" oriented groups (c) market oriented groups; (d) one-time operating groups (e.g., Brinks and Purolator robberies); (e) computer crimes; (f) other sophisticated crimes/capers.

C Politically motivated, issue oriented acts of violence or criminality -- normally of symbolic nature. Differentiated from terrorist acts in that violence is generally low level. Terror is not an objective.

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc.

E This group also includes former employees

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime.

SCALE:

Very Low — Low — Moderate — High — Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
BEHAVIORAL CHARACTERISTICS						
9. Motivation	Political and Ideological Hatred of Society (nihilists)	Financial gain and increased personal power	Politically-centered and issue-oriented Often result of frustration, discontent, anger, etc	Wide "range" Is a function of the individual's mental disorder	"Range" of employment - related problems (e.g., being fired, passed over for promotion, etc.)	Financial gain Desire for drugs and alcohol
10. Dedication/ Discipline	"Very High"/"Moderate"	"Moderate"/"High" (TOC) "Low"/"Moderate" (WCC & CC)	"Moderate"/"Moderate"	"Very High"/"Very High" (psychotic) "High"/"Low" (neurotic) "Low"/"Low" (anti-social)	"Low"/"Low"	"Low"/"Low"
11. Willingness To Kill	"Very High"	"Moderate" (TOC) "Very Low" (WCC & CC)	"Low"	"Very High" (psychotic) "Moderate" (neurotic) "High" (anti-social)	"Low"	"Moderate"
12. Willingness To Give Up Life	"High" - not generally suicidal but willing to give up lives for cause if required.	"Low" (TOC) "Very Low" (WCC & CC)	"Very Low"	"High" (psychotic) "High" (neurotic) "Very Low" (anti-social)	"Very Low"	"Low"

A. Examples include Baader Meinhof Gang, Red Army Faction, PLO, Red Brigades, IRA, SLA, FALN, Anti-Castro Cubans, etc.

B Examples include (a) traditional "family" oriented groups (e.g., Mafia in Chicago); (b) ethnic "family" oriented groups (c) matrix oriented groups; (d) one-time operating groups (e.g., Brinks and Purolator robberies); (e) computer crimes; (f) other sophisticated crimes/capers.

C Politically motivated, issue oriented acts of violence or criminality -- normally of symbolic nature. Differentiated from terrorist acts in that violence is generally low level. Terror is not an objective.

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc.

E This group also includes former employees.

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime.

SCALE:

Very Low — Low — Moderate — High — Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
RESOURCE CHARACTERISTICS						
13. Training/Skills	"High" levels of training in weapons use, tactics, explosives manufacture, forgery, codes, security, etc	"High" levels of training from Criminal experience (TOC) "High levels of college and technical training (WCC & CC)	Domestically, a range of informal group training and use of criminal experience.	Wide "range " Is a function of adversary's background, training and experience.	Wide "range " Is a function of individual's background, training and experience	"Low" levels of formal training "Street wise" criminal experience
14. Personnel Technical Sophistication	Typically "Moderate" Explosive device technical knowledge "High"	"Very High" with high levels of ingenuity and improvisation	"Moderate"	Wide "range " Is a function of individual's background, training and experience.	Wide "range " Is a function of individual's background, training and experience	"Low" Use of simple and unsophisticated techniques
15. Group Size	Typically 1-6	Typically 1-6	1-4 covert crimes Up to 35,000 mass/violent demonstrations (Western Europe)	Psychotics and Neurotics typically operate alone Anti-social operates alone or part of criminal group (size indeterminate).	Typically 1-2 6 or more in strike related crime	Typically operate alone Occasionally in groups of 2-5
16. Weapons	Handguns, rifles, shotguns, automatic weapons, explosives, grenades, anti-tank weapons, surface-to-air-missiles, chemicals and poisons	Handguns, rifles, shotguns, automatic weapons and explosives (TOC) None documented (WCC & CC)	Handguns, rifles, shotguns, explosives and incendiaries	Handguns and other small arms, explosives and incendiaries, objects of convenience	Handguns and other small arms, explosives and incendiaries, objects of convenience	Handguns and other small arms
17. Equipment	Simple tools for barrier penetration False documentation Communication equipment	Sophisticated security system bypass and physical barrier breaching equipment Other sophisticated improvised equipment	Protective helmets, gas masks, wire and bolt cutters, basic communications equipment, etc for mass/violent demonstrations Simple breaking and entering equipment and false ID for covert acts.	"Range" of equipment Is a function of individual's background, training and experience	"Range" of Equipment Is a function of individual's background, training, and experience Use of items of convenience in work area.	Simple breaking and entering equipment Low level explosives for penetration
18. Transportation	Private and leased vehicles, stolen vehicles, commercial aircraft, railway, small boats, motorcycles, on-foot	Private or leased vehicles, stolen vehicles, public transportation, privately owned aircraft	Privately owned vehicles, public transportation, motorcycles, on-foot, hitchhiking	Privately owned vehicles, public transportation, aircraft, on-foot.	Privately owned vehicles, public transportation, on-foot	Privately owned and stolen vehicles, public transportation, on foot

A Examples include Baader-Meinhof Gang, Red Army Faction, PLO, Red Brigades, IRA, SLA, FALN, Anti-Castro Cubans, etc.

B Examples include (a) traditional "family" oriented groups (e.g., Mafia in Chicago); (b) ethnic "family" oriented groups (c) matrix oriented groups; (d) one-time operating groups (e.g., Brinks and Purolator robberies); (e) computer crimes; (f) other sophisticated crimes/capers.

C Politically motivated, issue oriented acts of violence or criminality - usually of symbolic nature. Differentiated from terrorist acts in that violence is generally low level. Terror is not an objective.

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc.

E This group also includes former employees.

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime.

SCALE:

Very Low — Low — Moderate — High — Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1