A BEHAVIORAL ANALYSIS OF THE ADVERSARY THREAT TO THE COMMERCIAL NUCLEAR INDUSTRY—A CONCEPTUAL FRAMEWORK FOR REALISTICALLY ASSESSING THREATS

Phillip A. Karber and R. W. Mengel

BDM Corporation, McLean, VA 22101

Behavioral science has played a less than significant role in the field of physical security and security systems. There are some notable exceptions such as airport security, but on the whole the effort to apply behavioral science has not been monumental and its impact spotty. In part, the lack of application of behavioral science to physical security is a direct reflection of a clientele who does not understand or appreciate the role that behavioral science might play in solving security problems. The form and substance of behavioral science, requiring a multi-disciplinary approach, is beyond the average layman in most cases. The result of this reluctance to accept behavioral science as a viable approach to defining security requirements has been the infrequent use of this valuable tool.

The value in a behavioral approach to physical security issues lies in the very aspect that has limited its use, its multi-disciplinary nature. Critics of the behavioral approach stress that the behavioral sciences cannot solve security problems, failing to provide a real-world perspective. These same critics use the intuitive approach to security, emphasizing those factors related to the physical aspects and the application of resources to deterring, preventing, and responding to malevolent activity. Many of those that spurn the behavioral approach are also those that maintain that physical security systems can provide 100 percent assurance against any attack. In reality, there is no circumstance that will ensure 100 percent physical protection.

The behavioral approach provides a methodology by which physical security might be examined across the range of subjects that impact upon its success or failure. Combining systems analysis and behavioral approaches, one is able to examine physical security from the requirements definition phase through test and evaluation and implementation of a security system. The behavioral approach provides a methodology which is flexible enough to explore not only system vulnerabilities but also adversary resources and adversary motivations in terms of their inner relationships in a particular environment.

Over the past several years, the professional staff at BDM has been developing various aspects of the behavioral approach to physical security. In a recent contract for the Nuclear Regulatory Commission's Special Safeguards Study, the BDM project team developed and used a behavioral methodology to arrive at the terrorist threat to the commercial nuclear industry. In fact, this methodology provides a basic framework within which any threat analysis might be undertaken. This presentation offers a conceptual framework within which threats might be assessed realistically regardless of the environment. In applying this methodology to the nuclear industry it became apparent that its utility went far beyond that particular industry or the environment within which that industry is currently operating. In order to provide an operational setting to discuss a behavioral methodology, this presentation uses the nuclear industry to provide substantive examples.

METHODOLOGICAL FRAMEWORK

The basic framework for this behavioral approach to assessing threats is founded on seven questions which, when examined, provide a complete threat assessment. Each of the seven

questions requires the application of one or more of the behavioral di- plines in order to arrive at conclusive answers, the extent to which any one is used dependir on the specific threat being analyzed and the availability of information. When each of the seven questions has been answered individually, an overall analysis is undertaken to arrive at a composite threat assessment. The seven questions to be addressed in this behavioral framework are as follows:

(1) What are the identifiable characteristics of groups viewing nuclear facilities as targets and special nuclear materials (SNM) as potential weapons?

(2) What are the courses of "nuclear action" likely to be pursued?

(3) What are the likely objectives of a group and their correlation with possible courses of "nuclear action?"

(4) Considering past terrorism, what force level, knowledge, sophistication, etc., can be expected in an attack?

(5) Are the tactics, force levels, etc., likely to be used consistent with "nuclear action" objectives, tactics, etc.?

(6) What are the means for demotivating groups from nuclear violence?

(7) Why have there been no theft or sabotage attempts against licensed plants?

In the subsequent discussion each of these seven questions will be examined in terms of the approach taken and the types of conclusions that might be drawn.

QUESTION 1: WHAT ARE THE IDENTIFIABLE CHARACTERISTICS OF GROUPS VIEWING NUCLEAR FACILITIES AS TARGETS AND SNM AS POTENTIAL WEAPONS?

The approach to Question 1 involves three steps. First, a review of nuclear related activities was undertaken to include a comprehensive analysis of actual malevolent actions, an analysis of a selected set of threats against the nuclear industry and an evaluation of statements of expressed nuclear interest which, in this case, consisted of a content analysis of over 200 terrorist publications. Second, each of these activities was examined in light of the three primary identifiable characteristics, group, target, and type of attack. Third, the activities and the identifiable characteristics were correlated with comparable analyses of non-nuclear incidents. The purpose of this latter step is to derive any pertinent information that might be available from analogous threat situations.

The review of the events themselves does not merit further discussion at this point, but some of the insights that were derived from an examination of the three primary identifiable characteristics of the incidents are important for understanding the utility of a behavioral framework. The following insights are indicative of the range of salient information that might be derived from this first step in the conceptual framework.

(1) Insider assistance is critical to covert theft.

(2) Individual motivations are difficult to determine, while in many instances specific group motivations or objectives can be ascertained.

(3) There is high interest in low casualty-potential materials, while there appears to be less interest in high casualty-potential materials.

(4) The nuclear mystique affects individual behavior but fails to appear in any of the literature reviewed.

(5) Opportunities for casual theft are available to personnel with access to materials.

(6) Out of three protest type attacks, in two instances the attacking group cited opposition to nuclear energy programs.

(7) Transnational criminals have been contracted to steal nuclear material.

(8) There is no evidence that terrorists have undertaken any actions to fabricate nuclear weapons or dispersal devices.

Although the illustrative insights offered above indicate that it is possible to draw a wide range of initial conclusions, there are limitations to this initial step, particularly when dealing with nuclear data. In the first place, one cannot extrapolate into the future from the nuclear data base, as the environment will undoubtedly change; new groups with different motivations and resources will arise; and in the future, there will be more opportunities to attack nuclear targets as the industry expands. Additionally, there is an incomplete data base of past incidents/threats and literature. To date, there is no significant "history" which might be analyzed and conclusions drawn. Recognizing these limitations with nuclear data, it then becomes necessary to go beyond purely nuclear activities and explore those malevolent actions which might be analogous either in terms of the target or the potential outcome for such an attack. For the nuclear industry there are four analogies on which one might base further analyses. Figure 1 depicts the elements of the conventional-nuclear analogy. With this as a basis, it is possible to look at other activities and industries and derive germane conclusions. This type of approach, that of determining analogous situations, has utility in any threat assessment endeavor.

Type of salient characteristic	Analogy to nuclear installations	Method of analysis	Examples
High technology targets	A. Valuable or irreplaceable equipment B. Complex scientific apparatus C. Symbolic of modern technology	Collect and analyse violent acts perpetrated against computer centers, scientific laboratories, communications networks, etc.	Mass bombings of microwave transmission towers in U.S. Western States in 1960's
Energy systems	A. Produce public power B. Salient target for those interested in disruption outside the plant	Collect and analyse violent acts perpetrated against public power plants, dams, waterworks, and fuel depots	Mass bombings against public utility plants in California 1970-1972
Protected	A. Plants protected by fences B. Armed guards on duty C. Critical areas with controlled access	Collect and analyse violent military bases, banks, and guarded shipments	Arms thefts during early 1970's
Characteristics of past attacks	A. Types of groups committing acts in the past are likely to continue a trend of violence B. Inclination toward inflicting indiscriminate mass casualties	Review past behavior of known terrorists, criminals, avenging persons, dissident employees, etc., to identify propensities toward nuclear action	Inability of U.S. left-wing protestors to inflict mass casualties on the U.S. population during 1960's

FIGURE 1. *Elements of conventional-nuclear analogy.*

At the foundation of this behavioral approach to threat assessment is the determination of the relationship between the key variables and the questions which compose the basic framework. Figure 2 provides a graphic illustration of the relationships which exist between the key variables and the questions which are the heart of the methodology. In analyzing each of the questions, the triangular relationship between the key variables must be borne in mind. In taking a total approach to the problem of threat assessment, it is important to keep in mind that neither target vulnerability nor motivations nor resources/capabilities are stand-alone factors. Rather, it is necessary to examine all of these variables in such a way that the contribution of the multi-disciplines of the behavioral sciences are brought to bear on the question.

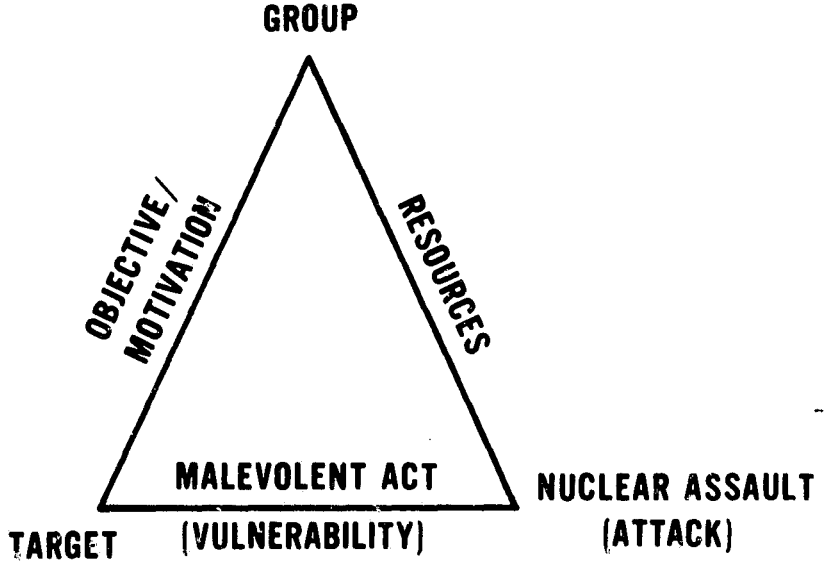

FIGURE 2. *Key analytic relationships.*

By way of explanation of figure 2, a brief description of the relationships between the various points and connecting lines of the triangle is desirable. The type of attack and the target are related by the vulnerability of that target. In other words, the type of attack necessary to overcome the target and achieve desired objectives is, in the main, determined by the vulnerability of that target. The relationship between target and group focuses on the motivation of that group. In order for a target to be attractive to the group, the target must offer a means to an end or help the group in achieving its objectives. The relationship between the group and type of attack is one of resources or capabilities. For example, if the group does not have weapons and ammunition available to it, the likelihood of an armed attack is very low.

The fifth question, which focuses on correlating motivations, resources and target vulnerabilities, will provide insights into the overall range of threats and the relative likelihood of any point on that range actually occurring. Questions 6 and 7 derive data from the relationships which are established between the key variables and, thus, depend upon the various facets of a multi-disciplinary approach to arrive at those elements which might demotivate potential attackers and arrive at an understanding as to the causes behind any current or past malevolent activities against a specific industry or set of targets. In this case, there was a desire to ascertain the means of demotivating individuals or groups from attacking the nuclear industry and ascertaining why there have not been any attacks of significance to date.

The empirical basis upon which BDM conducted this threat assessment to the commercial nuclear industry is a data base of approximately 5,000 malevolent acts collected for the period 1965 through 1977. This data base, consisting of 148 variables, primarily focuses on U.S. domestic and international terrorist activities. The data collected are multi-disciplinary in nature to include variables which depict motivation, resources, tactics, group characteristics, target characteristics, literature content, and profiles of known terrorists. This data base provided empirical support to the threat assessment, removing much of the analysis from the subjective/intuitive and placing it in the realm of the objective.

QUESTION 2: WHAT ARE THE COURSES OF "NUCLEAR ACTION" LIKELY TO BE PURSUED?

Question 2 focuses on the likely courses of nuclear action, i.e., acts of nuclear terrorism, likely to be followed by terrorists or other malevolent actors. Thus, this question attempts to identify the range of threats against the nuclear industry. In the past, three alternative approaches have been commonly used by those who have studied and postulated ranges of threats to the nuclear industry. Many practitioners of threat assessment have chosen the intuitive approach which permits a heuristic look at the range of threats. However, inherent in the intuitive approach are the disadvantages that there is a tendency to invent the maximum threat; non-explicit assumptions are made; internal inconsistencies between various levels of threat usually abound; and there is generally no evidential basis for the various threats. Second, the empirical approach attempts to identify key characteristics and establishes relationships between these characteristics. This approach, based on empirical data, tends to dispel myths which occur in threat assessments. The disadvantages of the empirical approach are that the past may not be a prologue to the future and is not predictive; there is a possibility that the sample might be biased and the validity of any subset questionable; and the majority of the data are overwhelmingly conventional, not nuclear. The third approach, the one which this conceptual framework is based upon, is behavioral analysis. This approach permits the manipulation of characteristics and the extrapolation from past data into future contingencies. The disadvantages of the behavioral approach tend to dissipate when they are combined with empirical and intuitive research. In essence, it is recognized that any behavioral effort cannot do without empirical data or the subjective judgments which form the basis for substantive conclusions.

The approach taken within the conceptual framework to examine Question 2 has been to, first, review the hypothesized attacks which have resulted from previous intuitive and empirical analyses. This created certain problems with identification of the range of threats in that only the worst threats were completely evident; it was difficult to rank the threats on a continuum, and there was no way to establish the likelihood of occurrence. From this review, it became obvious that a different approach to the question was required. From this initial review of hypothesized attacks, it was determined that the first step was to differentiate the various acts of nuclear terrorism. Once this was accomplished, it was then possible to rank these attacks according to their severity in terms of consequences to the general public. Following this ranking, it became necessary to develop the attack sequence in order to define the relative likelihood of any one occurrence. Once this attack sequence had been developed, it was then possible to identify the generic tasks involved in an attack. Drawing the above steps into a final phase, a comparison of the nuclear attack to analogous conventional malevolent actions was undertaken.

The different acts of nuclear terrorism were determined using past experience within the nuclear industry, the hypothesized attacks reviewed earlier, and a general analysis of the types of actions that might be undertaken against the nuclear industry. The different acts of nuclear malevolence are outlined and ranked in terms of attack severity in figure 3. This severity was measured in terms of the consequential public casualties for each of the acts undertaken. Although highly judgmental in nature, the determination of public consequences on a relative basis provided a means of analyzing and ranking severity.

In a separate but related step, the sequence of the attack was developed, examining the degree of penetration which was required to perpetrate the various acts of nuclear malevolent actions. The facility was generically drawn with the respective barriers indicating a level of penetration. Each of the acts of nuclear malevolent action was in turn evaluated against the schematic to arrive at a necessary and sufficient level of penetration for each act (fig. 4). Once this had been accomplished, the number of generic tasks involved in each attack was differentiated. This provided a basis for drawing conclusions concerning the attack sequence and its relationship to the nuclear industry. These conclusions include:

(1) The deeper the penetration into the facility, the greater the number of generic tasks that are required.

(2) The deeper the penetration, the greater the variety of generic tasks that are required.

(3) The deeper the penetration, the greater the number of concurrent tasks that are required.

(4) Thus, the deeper the penetration, the greater the resources required in terms of personnel, knowledge, and equipment, and the greater the degree of motivation (dedication).

There are a series of conclusions that can be drawn from the examination of the courses of actions likely to be undertaken by a malevolent actor. First, over 95 percent of the incidents examined in the nuclear industry would fall within the purview of industry, rather than posing a general safeguards problem to the public. Second, there are no incidents recorded which substantiate the establishment of any relationship between venting, dispersal and fabrication and conventional attacks in terms of public consequences. Third, in those instances when the danger to the public is consequential they are acts which involve hostage, theft and damage situations. By comparison, the number of situations of this type is extremely low.

- Hoax—dupe or trick
- Threat—expression of intent
- Harassment—limited to exterior facility
- Disruption—interruption of facility operation
- Hostage—disruption by hostile presence
- Damage—significant destruction of key facility component
- Venting—release of radioactive material on site
- Theft—material diversion outside facility
- Dispersal—release of radioactive material into public domain (off-site)
- Fabrication—development of a nuclear device with the threat to endanger public safety

FIGURE 3. *Range and rank ordering of malevolent actions.*

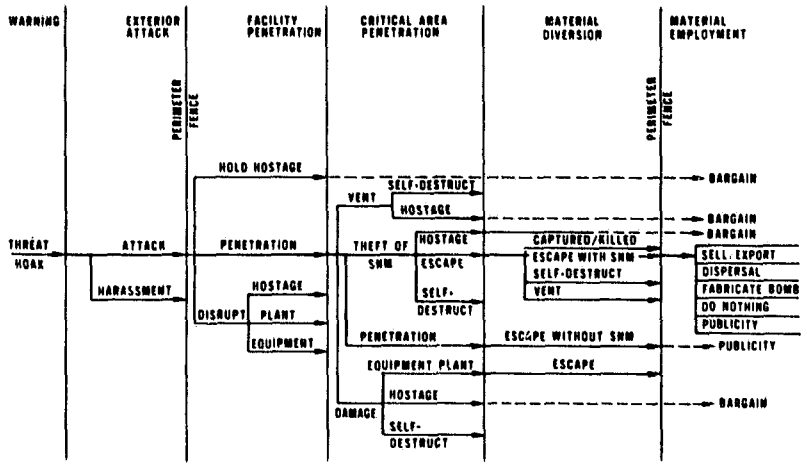

FIGURE 4. *Sequence of facility penetration and range of malevolent actions.*

QUESTION 3: WHAT ARE THE LIKELY OBJECTIVES OF A GROUP AND THEIR CORRELATION WITH POSSIBLE COURSES OF "NUCLEAR ACTION"?

Since any discussion of objectives of acts and motivations must, in and by itself, be highly detailed and involves complex studies of both group behavior and individual psychology, it is the intent of this discussion to merely highlight the approach taken to this question and provide some of the conclusions which were derived from the analysis of the nuclear industry. The approach to Question 3 is essentially twofold. In the first instance, a typology of violence approximating the objectives of likely attacks on nuclear facilities was constructed. This typology included a general violence classification which was theoretically based; a description of private versus public objectives; and an analysis of the forms of terroristic violence. The second step in this approach to motivation is the establishment of the relationships of the forms of violence to types of attack (courses of nuclear action), targets, groups, and environment.

The forms of violent behavior can be divided into two general categories with respect to motivations. On the one hand are the private motivations which include criminals, avengers, psychopaths, and vigilantes. In the other instance are those forms of violent behavior which are ascribed to public motivations and include terrorists, protesters, psychopaths, and paramilitary organizations.

In analyzing the forms of terroristic behavior, one finds that there is a relationship between target selection and the motivations/objectives of the perpetrators. Specifically, figure 5 depicts the relationships between instrumental and affective behavior and random or selected targets. In the case of random and selected targets, they might further describe these as either discriminate (selected) or indiscriminate (random) targeting. One can see from this paradigm the relationship between target selection and the instrumental or affective objectives of the group. As the objective of the group becomes more severe in terms of societal consequences, the targeting tends to move

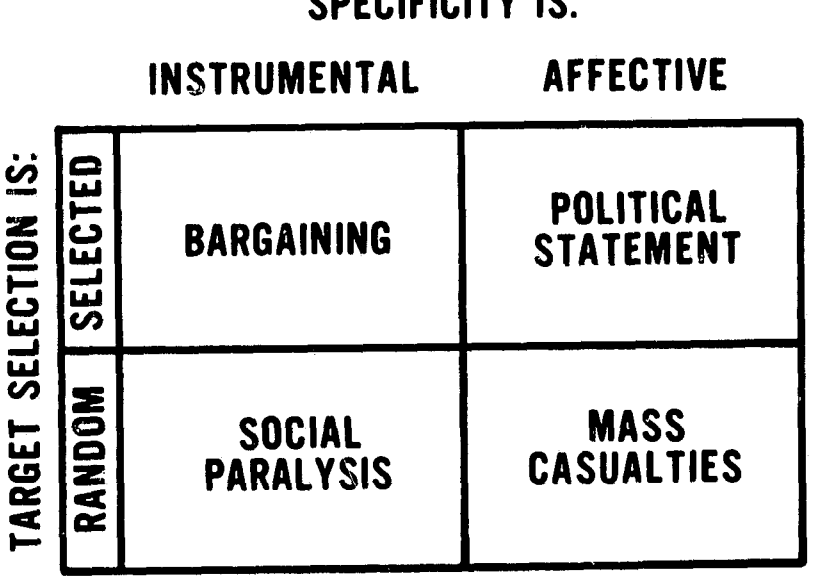

FIGURE 5. *Typology of terrorist behavior motivations.*

from discriminate and instrumental to indiscriminate and affective. For the nuclear industry the significance of this analysis lies in either the presence or the absence of the professed objectives which would tend to fall in the indiscriminate affective end of this violence paradigm.

In the course of studying motivations and possible nuclear actions several conclusions were drawn. The most significant conclusion is that generally groups have not been motivated to inflict mass casualties. This has a direct correlation and relationship to the nuclear industry. Second, individuals and groups tend to avoid confrontation which could result in death to the attacker. This is reflected in the high number of discriminate instrumental target attacks which have a low possible consequence for the attacker. Third, groups have not been motivated to attack high technology targets such as nuclear power plants, refineries and chemical complexes. Rather, groups have concentrated on highly symbolic targets such as governmental and military installations which convey a message related to the objectives of the group. Fourth, for one or two individuals engaged in violence the primary motivations have been revenge. For larger size groups, the primary motivations have been disruption, protest or simple demonstration.

QUESTION 4: CONSIDERING PAST TERRORISM, WHAT FORCE LEVEL, KNOWLEDGE, SOPHISTICATION, ETC., CAN BE EXPECTED IN AN ATTACK?

An equally important aspect of threat assessment focuses on the nature of resources available and the modus operandi of malevolent actors. Resources are one of the key components in the analysis of any threat and when correlated with motivations and target vulnerability provide the broad base necessary for complete and incisive threat assessments. The approach taken to this question is predicated on three prerequisites for a successful attack. These prerequisites are organization, training, and level of force. Specific sub-categories under each of these are depicted below:

- Organization
  - discipline
  - detailed planning
  - knowledge of target
- Training
  - tactical weapons
  - sophistication
- Level of Force
  - people
  - weapons
  - special equipment

Using these three prerequisites to a successful attack, empirical indicators of resources have been developed. For organization such items as motivational commitment, previous similar experience, and inside collaboration are useful as indicators. For measuring training as a resource one can look at the types of task involved in attacks and previous evidence of number of tasks, different tasks, and concurrent tasks in malevolent activities. With respect to level of force it is possible to empirically measure that resource by examining the number of personnel involved in previous attacks, the types of weapons and equipment used and access to and utilization of special equipment.

A few of the findings from the nuclear industry threat assessment merit mention at this point. In reviewing the frequency of attack sequences, it was found that in 70 percent of the attacks only a primary task was accomplished. For example, the placing of a bomb against a window or door outside a building involves only one primary task. In 25 percent of the cases, there were secondary tasks involved, such as entry into a building and then the placement of a device. In only 40 percent of the cases were there three tasks involved and in less than 1 percent four major tasks involved. Equally revealing are the empirical indicators related to personnel resources used in attacks. In over 95 percent of the incidents examined, three or less perpetrators were involved. This indicates that in the majority of the attacks there was a relatively small force

to be dealt with. The data on frequency of equipment usage in attacks reveals that small arms and explosives are used in the vast majority of all incidents while the occasions in which automatic weapons, crew-served weapons or communications equipment are found is limited to less than 5 percent of the cases.

From this analysis of resources it became evident that there are restraints on resources which impact on the ability of a perpetrator to undertake an attack. Specifically, the environment may limit the availability of resources to an individual or group. Second, a target may be invulnerable to overt attack because of the restraints on resources to a specific group or individual. Third, there are a series of invariant characteristics of a group which, in and by themselves, are limiting in terms of resources: there is a finite limit of force which can be brought into any one organization; the level of force is easier to change than the level of training of the perpetrators; the level of training is easier to change than the organizational structure necessary to accommodate an increase in force beyond a certain level.

A series of conclusions concerning resources was arrived at with respect to the nuclear industry. These conclusions are summarized below:

(1) Very few groups, particularly those engaged in terrorism, have the organization, training, or level of force necessary to carry out an attack against the nuclear industry with major societal consequences.

(2) Those terrorist groups that have the resources to attack a nuclear target, such as a number of international groups, have not operated, to date, in the U.S. socio-political environment.

(3) There are a number of non-terrorist groups potentially capable of operating in the U.S. that have the requisite resources to successfully attack nuclear targets and include a group of insiders, organized criminals, and military adventurers.

QUESTION 5: ARE THE TACTICS, FORCE LEVELS, ETC., LIKELY TO BE USED CONSISTENT WITH "NUCLEAR ACTION" OBJECTIVES, TACTICS, ETC.?

Question 5 provides the basis for exploring the correlations between the respective primary variables in the framework: resources, motivations, and vulnerability. The approach to this element of the framework consists of a series of seven steps through which the information derived from the initial questions were further analyzed. Specifically, the seven steps are as follows:

(1) Identify the key relationships or malevolent actions between nuclear facilities and nuclear actions (Question 2).

(2) Correlate those malevolent actions with the range of attack—objectives identified in Question 3.

(3) Evaluate those malevolent actions in terms of consistency with resources identified in Question 4.

(4) Examine interaction between resources required and nuclear actions to determine whether they are sufficient to achieve a desired attack objective.

(5) Project the interrelationships between nuclear action and the conventional type of attack which would be employed against the nuclear industry.

(6) Identify the range of potentially threatening types of groups which could possess the resources and have the objectives (motivations) required to undertake a terrorist type attack against a nuclear facility.

(7) Rank order those types of groups most likely to conduct terrorist type actions against the commercial nuclear industry or nuclear terrorism against the public.

The result of evaluations conducted through these seven steps should establish the key relationships between the types of malevolent action and nuclear facilities, the interactions

between resources and nuclear actions that affect the desired attack objective and the ultimate determination of the range of potential threatening groups and their rank ordering in the present social/economic environment.

In determining the key relationships between malevolent action and nuclear facilities, it was determined that nuclear power plants are likely to attract malevolent action which entail the facility serving as a hostage; the venting of radioactive material; or damage to the energy production capability. With respect to fuel fabrication plants the most likely malevolent actions are to be occupied to serve as hostage and to effect the theft of SNM. In analyzing reprocessing plants, it was determined that the likely malevolent actions include occupation in order to serve as a hostage and for the theft of SNM. Finally, transportation means are likely to attract malevolent action in order to effect the theft of SNM.

In viewing the interaction of resources and nuclear actions as they affect the desired attack objective, one finds that several conclusions can be drawn. First, if the attack objective is to gain publicity, it is likely that the attack will be upon the exterior, involving minimum resources in organization, training and level of force. Second, if the attack objective is to protest in some way, it is also likely that the attack will be upon the exterior of the facility and involve minimum resources in terms of organization, training and level of force. Third, in bargaining situations a penetration of the facility would be required, calling for an attack force of more than three persons and levels of equipment which would include explosives and small arms. These three examples are indicative of the types of analyses and resultant conclusions that would take place in determining the interaction of resources and nuclear actions in order to achieve a desired attack objective.

Given the present social/political environment within the United States, a rank ordering of potentially threatening groups is illustrated in figure 6. As can be seen in the rank ordering presented in figure 6, organized criminals are the most threatening group in terms of resources, capabilities and motivations. Following criminal groups are dissident employees, which is indicative of the target knowledge and target access that employees would have. Following the criminals and dissident employees in order of perceived threat are the transnational terrorist groups followed by domestic issue-oriented groups and domestic terrorist groups. Figure 7 provides a graphic portrayal of the attributes necessary to pose a safeguards problem. This same methodology might well be used in assessing any set of threats to any industry. Paramount in this assessment of the three primary attributes, motivation, target vulnerability as reflected in past targets attacked, and resources, is the ability to bring to bear the full range of behavioral sciences to include psychology, sociology, political science and human factors.

1. Organized criminals
2. Dissident employees
3. Foreign/transnational separatists
4. Foreign/transnational revolutionaries
5. Issue-oriented
6. Black revolutionaries
7. White revolutionaries
8. Right-wing extremists

FIGURE 6. *Rank order of potentially threatening groups in the present socio-political environment.*

Characteristic		Target characteristics				Resources				
Type of group	Motivation	Mass casualty	Protected	Hi-tech	Energy	Training	Organization	Knowledge	Force	Remarks
Criminal			X			X	X	X	X	If market is established becomes primary threat-theft
Dissident employee	X		X					X	X	Most inspection threat because of inside position
Foreign separatist		X	X			X	X		X	Lacks motivation to attack U.S. nuclear industry
Foreign revolutionary			X		X	X	X		X	Lacks motivation to attack U.S. nuclear industry
Separatist		X	X				X		X	If motivated, mass casualty potential may make nuclear industry a target
Revolutionary			X				X		X	Motivation and overall resources lacking today
Violent issue-oriented				X			X	X		No motivation to create a safeguard danger
Reactionary extremist						X	X		X	No motivation to attack industry, no common threats
Sociopathic										No threat
Ad hoc	X				X					May be industry threat
Individual	X		X		X					Industry threat
Anarchist										No data on this type of group in the U.S.

FIGURE 7. *Attributes necessary and sufficient to pose a safeguard problem.*

QUESTION 6: WHAT ARE MEANS FOR DEMOTIVATING GROUPS FROM NUCLEAR VIOLENCE?

The question of means available for demotivating groups and individuals that are in pursuit of nuclear violence must focus on the full range of the behavioral disciplines. It is not satisfactory to state that target protection will be increased to the point that the target is invulnerable to attack. In most situations this approach is totally inadequate and unrealistic. The fact of dollar constraints forces those persons responsible for physical security to do a cost-benefit analysis in terms of what can be protected against realistically versus what can be afforded. Demotivation in a dollar constrained environment takes on even greater significance as it might be cheaper to demotivate than to spend recurring dollars on physical security. The basic approach to Question 6 is to determine what elements in the triangular relationship can be altered to enhance the opportunities for enhancing target protection. This does not necessarily mean that target security must be physically enhanced, but rather, those segments of the triangular relationship which can impact upon motivation and availability of resources must be identified and acted upon.

The key variables of resources, motivations and vulnerabilities can be altered in order to achive demotivation. In looking at each of these variables, examples of demotivating changes can be cited. In the case of motivation/objectives it is possible to exercise adaptation, alienation, legitimization of demands and actual educational campaigns. In the case of resources, it is possible to infiltrate the group with informants, establish weapons control systems, improve personnel security systems, and establish critical equipment controls. In terms of demotivation through changing the vulnerability variable, it is necessary to improve physical security to the point that outside attackers will view the situation as having a greater risk than potential attractiveness.

A series of conclusions can be reached concerning demotivation and countermeasures. First and foremost, the most difficult linkage to break in the triangular relationship is motivation. In order to alter the motivation of a group, one must primarily rely on altering the group's perception of risk versus attractiveness. Second, resources cannot be denied malevolent groups or individuals in general, but certain resources critical to handling of SNM can be monitored and perhaps restricted. Third, 100 percent target invulnerability is not possible, but systems that contain repetitive security measures, or security in-depth will deter most attackers. Fourth, intelligence must be able to provide information on the unanticipated threat and changed environment. Although most difficult in today's milieu of enhanced personal privacy and expanded freedom of information, intelligence is still a key variable in preventing and deterring threats.

QUESTION 7: WHY NO THEFT OR SABOTAGE ATTEMPTS AGAINST LICENSED PLANTS?

As a final step in this conceptual framework, it is necessary to ask the question, why have there been no attempts of theft or sabotage of licensed nuclear facilities? This same question might be posed in any threat assessment, either to determine the level of threats that have occurred to date and ascertain why that level has been reached or to explore why there have been no previous threats. In either case, the results of this question should provide the analyst with some idea as to the future potential for threats and the level to which these threats might rise.

The approach to this question is to hypothesize, using analogies and social indicators, the environments which might be favorable to an attack. As a second step, one should project the groups or individuals that are most likely to mount an attack. As a third step, it is necessary to project the objectives, resources, and consequences of an attack. In doing this, one must be able to postulate and examine the types of attack that are likely and the consequences of those attacks. At the final step in the approach to resolving Question 7, it is necessary to generate the variables that are representative of the projected environments. The accomplishment of this fourth step will permit the threat analyst to identify those variables which are primary and secondary in future environments.

By way of illustration, for the nuclear industry, five specific environmental variables were identified and the motivations, resources and consequences of an attack were examined in terms of each. These five environmental variables included:

- Group antagonism environment
- Domestic environment
- Interstate environment
- Interstate nuclear environment
- Nuclear technology environment

Each of these in turn was examined in terms of the change in the environment which must take place and the potential type of malevolent action which might result should a group undertake an attack. In answering Question 7, one has, in essence, examined the range of potential future threats to the industry.

END