BNL-71383-2003-CP

Terrorist Protection Planning Using a Relative Risk Reduction Approach*

Session VIII: Technology Forum Focus Groups

Dr. Joseph P. Indusi
Nonproliferation and National Security Department
Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000

Phone: 631-344-2975
Fax: 631-344-5266
E-mail: indusi@bnl.gov

*This work was performed under the auspices of the US Department of Energy, Contract No. DE-AC02-98CH10886.

TERRORIST PROTECTION PLANNING USING A RELATIVE RISK REDUCTION APPROACH*

ABSTRACT

Since the events of 9/11, there have been considerable concerns and associated efforts to prevent or respond to acts of terrorism. Very often we hear calls to reduce the threat from or correct vulnerabilities to various terrorist acts. Others fall victim to anxiety over potential scenarios with the gravest of consequences involving hundreds of thousands of casualties. The problem is complicated by the fact that planners have limited, albeit in some cases significant, resources and less than perfect intelligence on potential terrorist plans. However, valuable resources must be used prudently to reduce the overall risk to the nation.

A systematic approach to this process of asset allocation is to reduce the overall risk and not just an individual element of risk such as vulnerabilities. Hence, we define risk as a function of three variables: the threat (the likelihood and scenario of the terrorist act), the vulnerability (the vulnerability of potential targets to the threat), and the consequences (health and safety, economic, etc.) resulting from a successful terrorist scenario.

Both the vulnerability and consequences from a postulated adversary scenario can be reasonably well estimated. However, the threat likelihood and scenarios are much more difficult to estimate. A possible path forward is to develop scenarios for each potential target in question using experts from many disciplines. This should yield a finite but large number of target-scenario pairs. The vulnerabilities and consequences for each are estimated and then ranked relative to one another. The resulting relative risk ranking will have targets near the top of the ranking for which the threat is estimated to be more likely, the vulnerability greatest, and the consequences the most grave. In the absence of perfect intelligence, this may be the best we can do.

RISK CONCEPT

The concept of risk has different meanings depending on the context and individual. Here we use a logical or systematic definition based on the mathematical construction used in nuclear reactor safety and other physical systems. In this context, the risk is generally defined as

(1) $R = P \times C$,

where P = probability that a system failure occurs and C is an estimate of the consequences resulting from the system failure. The analyses of the various failure events and consequences associated with nuclear power reactors have been extensively studied and delineated.

*This work was performed under the auspices of the US Department of Energy, Contract No. DE-AC02-98CH10886.

In an effort to introduce the concept of risk to the design of nuclear materials safeguards systems, there evolved the formulation known as the Societal Risk Approach to Safeguards .[1] In this formulation, the safeguards risk is approximated by an equation of the form:

(2) $R = Pa \times (1-Pi) \times C$,

where Pa = probability that a person or group attempts an adversary action, Pi is the probability of adversary interruption (by the safeguards system), and C is an estimate of the consequences from the action. The implementation of this societal risk approach is problematic because of the difficulty in estimating the probability of attempt Pa. The situation for estimating the probability of interruption Pi and the consequences C is somewhat more amenable to analysis. Indeed, there has been significant progress in analyzing and quantifying both of these factors, at least in the case of nuclear facilities safeguards analysis. To cope with the difficulty in determining Pa and in an attempt to develop a useful formulation for protective system planning, we may use a less formal mathematical version of equation (2). In equation (2), we may think of Pa as the threat, that is, the element controlled by the adversary or terrorist group. The factor (1-Pi), the probability that the adversary is not interrupted, is analogous to the vulnerability (to the potential threat) of the protective system. Just as in equation (2), the consequences must also be considered. With these concepts, we now define risk as:

(3) R = Threat x Vulnerability x Consequences

which is estimated for each threat scenario at a given facility. A risk value for each threat scenario at a given facility may be analyzed to give a set of risk values for the given facility. Now these risk values may be ranked, relative to one another, from the highest to the lowest. Since there is no certainty or mathematical accuracy in developing the probability of attempt or threat, the risk values so derived are necessarily relative to each other.

RISK CONCEPT ATTRIBUTES

In the weeks and months following the attacks of 9-11, there were many calls for vulnerability, threat and risk assessments. Often, these terms were used with no standard or agreed meaning for each. In the risk formulation of equation (3), it is clear that each element has a meaning and the relationship between them is consistent and systematic. For example, using equation (3), a high risk implies a very plausible adversary scenario (threat), a target which is very vulnerable to the threat, and a severe set of consequences will occur if the threat is carried out. It should follow easily that upgrades or security plans should be based on risk and not on one or two of the elements of risk alone. Clearly, basing security upgrades on say vulnerability alone does not optimize the use of resources.

Unfortunately, upgrades in facility security were often based on vulnerabilities alone. Similarly, the general public tends to focus on high consequence events, even when other elements of the risk are low. The National Strategy for Homeland Security in its' July 22, 2002 report stated "Accordingly, the federal government will apply a consistent methodology to focus its efforts on the highest priorities". [2] In practice, a relative value, such as low, medium or high, can be assigned to the threat, vulnerability and consequences for each threat scenario. As in the case with equation (2), given a threat scenario at a given facility, we are capable of assigning relative vulnerability, and consequence values. In utilizing equation (3), the difficulty again lies in the threat element. Of course, with perfect intelligence, the threat can be neutralized before the adversary acts. However, in the absence of reliable threat intelligence, we must act prudently to use resources for the highest risk scenarios and targets.

To proceed, it is necessary to delineate the full spectrum of potential threats against a given target or facility. For purposes of homeland security, these targets are largely the elements of the critical infrastructure such as transportation (bridges, tunnels, aircraft), energy (pipelines, power lines, etc.), finance and banking and the others. Developing these threat scenarios requires that we focus on the future, integrating and analyzing available intelligence, and thinking in the ways an adversary thinks. This is part of the message given by Col. Randall J. Larsen, (USAF-Ret.), Director of the ANSER Institute for Homeland Security in his statement for the National Commission on Terrorist Attacks Upon the United States. [3] Similarly, the National Strategy also states "Mapping terrorist threats... against specific facility sectoral vulnerabilities will allow authorities to determine... which facilities and sectors are most at risk". The process of developing the threat scenarios will require participants from many disciplines and experiences, including historians, intelligence specialists, technical experts, and including military and law enforcement organizations. Once this formidable task is completed, the development of a relative risk ranking may proceed.

IMPLEMENTATION

Constructing a relative risk ranking begins with the list of threat scenarios against targets or facilities. Presumably this list may be small or large, but countable in number. While there is no guarantee of completeness, the mere act of developing threat scenarios is instructive in itself and provides insight into potential future threats. For each threat scenario, the vulnerability and consequences are then estimated. Fortunately, there are mathematical models to analyze both, developed in the nuclear safety and safeguards community and the military operation research community. These estimates may be qualitative such as low, medium or high. The exact values are not important for purposes of this analysis.

The risk values are then determined and ranked from the highest to the lowest producing a relative risk ranking. Obviously, resources should be used to reduce the vulnerabilities or mitigate the consequences from the highest ranked threat scenarios first. In the National Strategy for Homeland Security, it is stated "Protecting America's critical infrastructures thus require that we determine the highest risks... .".

In planning security upgrades at Brookhaven National Laboratory, a select committee was established and this relative risk ranking concept was used for ordering the upgrade schedule.

CONCLUSION

The relative risk assessment concept or approach for protection system planning provides a framework for systematically allocating resources. It avoids the tendency to focus only on one element of risk such as vulnerability. It also forces planners and protection managers to look to the future and identify potential threat scenarios. Given the current global threat of terrorism, we cannot continue the methods of the past or follow the path of business as usual.

REFERENCES

[1] "Societal Risk Approach to Safeguards Design and Evaluation", C. A. Bennett, W. M. Murphy, and T. S. Sherr, ERDA-7, 1975.

[2] National Strategy for Homeland Security, Office of Homeland Security, July 2002.

[3] Col. Randall J. Larsen, (USAF-Ret.) Director, ANSER Institute for Homeland Security, Statement for National Commission on Terrorist Attacks Upon the United States, April 1, 2003.