SAND2021-9663C

Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting

August 23-26 & August 30-September 1, 2021

Innovative Methods to Predict Future Nuclear Security Threats as the Basis for Regulatory Development

Sandoval, Joseph S.
Sandia National Laboratories

ABSTRACT

Responsible use of nuclear material includes ensuring that safeguards, security, and safety measures are implemented to protect people and the environment from its potential harmful effects. Effective security measures require implementation of measures to protect against people who might attempt to use the material for malevolent purposes. Evaluating threats involves identifying the types of individuals or groups of individuals who may attempt to commit a malevolent act, and then using that as the basis for developing a regulatory nuclear security framework. Predicting potential threats is difficult. Historical human events can be a poor indicator of future events. A lack of past events also may not indicate the possibility of future events. Limited resources make it impossible to protect against all possible threats, and regulatory developers must decide which threats to protect against. Expending limited resources to defend against potential threats, then failing to protect against unanticipated threats, is a failure of the regulatory framework. Two methods commonly advocated to address this issue are scenario planning and a probabilistic approach. Scenario planning involves evaluating the range of potential threats and identifying the most plausible threats and scenarios. In a probabilistic approach, prior data and future indicators are used to predict the likelihood of a specific threat to quantify its risk. Because each method has strengths and weaknesses, this paper proposes combining the strengths of the two methods to provide decision makers with both a range of potential future threats with methods to continuously evaluate which threats are more likely to emerge. If successful, this proposed method will support better allocation of limited resources to reduce overall security risk.

INTRODUCTION

In many fields, such as regulatory development for nuclear security, determining optimal protection measures is a prediction. It is a prediction based on a forecast of what the threats are, what their capabilities are, what their intent is, and what measures will provide adequate protection to prevent them. Historically, forecasting human actions with any certainty can be difficult.

In the 21st century B.C., the ancient Sumerians had a very advanced civilization, but they began to be threatened by the Amorites who were gaining in power. The Sumerians constructed a massive 155-mile-long barrier known as the “Amorite Wall” between the Euphrates and the Tigris rivers to protect themselves. It was effective for several years until the Amorites learned how to bypass the wall with their army, and along with the Elamites destroyed the Sumerian city of Ur, ushering in the eventual end of the Sumerian civilization. Although the wall was not effective for very long, it marked the beginning of the concept of fortifications or barriers as an important component of

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

protection, but also illustrated another concept, that all barriers can be defeated with enough time and resources.

On November 1, 1964, a small force of Viet Cong troops attacked the Bien Hoa Air Base near Saigon. They killed four troops, injured 30 more, and destroyed or severely damaged 20 B-57 bombers in a very short time. The attacking force escaped undetected, and the attack left behind damage out of proportion to the effort expended. At the time, the U.S. Air Force minimally protected their airbases, because they believed they were far enough removed from the front lines of the war to be attacked, and they would detect an enemy force moving towards an airbase. The success of the attack led to attacks of many other airbases. The Viet Cong had adopted Mao Tse-tung's concept of guerilla warfare as a way for a smaller, less equipped military to fight a larger, better equipped, but less flexible adversary [1]. They also espoused the ideas of Giulio Douhet, the Italian general and air power theorist, who said in 1921: "It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air" [2]. The failure to protect the base caused the U.S. to begin to change airbase defenses to adapt to the new threat, continuing the historical concept of a trial-and-error methodology.

One important lesson learned from the attack was that small unit attacks on semi-fortified sites requires careful and precise planning to have any possibility of success, which in turn requires a good deal of information about the site, its fortifications, its guards and weapons, and the intended target or targets of the attack. The Viet Cong relied heavily on an advance collection of intelligence gathered through espionage, ground reconnaissance, and electronic warfare (primarily intercepting, jamming, and imitative deception of radio communications) prior to their attacks.

This led to the idea that in addition to the importance of implementing additional passive defensive measures to defend a site against an attack, active security measures designed to deter, disrupt, and detect potential attacks before they occurred were just as important, if not more so, than passive defensive measures, because they could potentially prevent attacks before they occurred [3].

In both cases, the process has changed little. Security has historically been implemented by answering three basic questions:

1. What is the threat and what are their capabilities?
2. What is the threat's intent (What is the target)?
3. What measures are necessary to protect against the threat, and what are the consequences of failure?

Developing protective measures to answer the third question involves evaluating the threats, their capabilities, their intent, and developing plausible scenarios that could result in unacceptable consequences. Understanding the types of scenarios that may need to be defended against forms the basis for determining what measures are needed to protect against the threat. If an attack occurs, the effectiveness of the measures is determined by the outcome. Failure to protect may be due to:

- A misunderstanding of the threat or the threat capabilities
- A misunderstanding of the threat's intent (e.g., did not protect the right target)
- Failure to consider the right scenario (e.g., protected against physical access to a computer, but the threat gained access remotely)
- Ineffective protection measures

SCENARIO PLANNING AND PROBABILISTIC METHODS

Scenario planning is subjective, and if unconstrained, can be complex and discursive. The process is not predictive and requires a structured process to develop scenarios that are plausible given an understanding of potential threats and threat capabilities. One challenge is controlling the number of scenarios developed. Too few may lead to missed possibilities and inadequate protection, and too many, encompassing all possibilities without any boundaries and everything in between, makes it nearly impossible to make decisions and act.

This shortcoming is one of the drivers that leads to interest in probabilistic approaches. In the safety world where PRA techniques are ubiquitous, scenario planning is seen as too open ended and subjective to be useful and potentially misleading. In addition, after developing and visualizing a particular scenario, humans commonly exhibit confirmation bias, where plausibility is confused with probability, and they are prone to incorrectly see evidence of its emergence.

In many industries, such as nuclear energy and aerospace, significant potential consequences of failure led to development of methods to minimize failure as much as practical. The concept known in the aerospace industry as Fly-Fix-Fly in the 1940s, where aircraft were designed, built, flown until they crashed, and then improved, was deemed unacceptable when consequences of a failure could be catastrophic [4].

The potential consequences to the public and the environment from a failure at a nuclear power plant led the U.S. Congress in the 1970s to direct the Atomic Energy Commission to conduct a reactor safety study to determine how safe the plants were. The study (WASH-1400) was led by Professor Norm Rasmussen and a team from the Massachusetts Institute of Technology (MIT) [5]. The team developed the concept of societal risk and established the principles that underpin the probabilistic risk assessment (PRA) methods still widely used today. At a high level, the concept of the risk assessment was to answer three questions: (1) What can happen? (2) How likely is it to happen? and (3) If it does happen, what are the consequences? [6].

The concept of applying a modified probabilistic approach, based on the methods defined in WASH-1400, to evaluate the risk from an attack on a nuclear facility was proposed in 1975 [7]. The fundamental concept of risk as defined in WASH-1400 is that risk can be defined numerically as the product of the probability an event occurs and the consequence of the event. The proposed ERDA-7 risk equation added a third variable into PRA equation, the probability the system fails to protect against the threat. The approach was evaluated by Professor Rasmussen in 1976, and he determined it was flawed for many reasons [8]. ERDA-7 type approaches have been reintroduced, used, and evaluated many times over the years. The evaluations continue to reach the same conclusion as Professor Rasmussen, that the approach is problematic [9, 10]. The challenges and drawbacks of attempting to use a modified PRA approach in security were deemed significant for many reasons, most notably that a human plans, behaves, makes decisions, and takes actions that are difficult to predict, and are not random. Additionally, there are significant issues in attempting to predict the probability of an attack by a given threat. However, studies indicated some of the methods associated with PRAs could be used to implement a systems approach, to better develop a plausible range of threats and scenarios, and to evaluate and understand the dependencies, uncertainties, unknowns, and assumptions that form the basis of an analysis of the effectiveness of protection against [11].

PRA type techniques are much less subjective than scenario planning methods and rely on data and calculations to support results. Deductive approaches use models or laws that describe behaviors of a system, while inductive approaches simply use data to predict future events, since a key assumption is the future will resemble the past. This leads to a shortcoming of the methods in the security world when there is little or incomplete data. Accurately predicting human behavior has largely eluded prevailing models, data is often unavailable or unprecedented, and countless variables interact in infinite ways. Human decision-making and behavior can be illustrated in a decision tree with branching paths. Since each decision can result in multiple possible outcomes, the tree can become increasingly complex after a few branches, with exponentially increasing uncertainty. In addition, actions of a person function as a series of events based on which paths are chosen at each branch, and many times the decision to choose one branch over another is based on chance or coincidence. Sometimes significant events can result from a series of seemingly unrelated, mundane choices, making deducing human decision-making and behavior from past events difficult.

The scenario planning method and the probabilistic approach each have fundamentally different assumptions about the future. Scenario planning is based on plausibility, not probability. In a probabilistic approach, the intent is to determine the probabilities of different outcomes, turning uncertainty into quantifiable risk. In many fields, the benefit of being able to realistically estimate the probability or likelihood of possible future events is significant. The challenge with probabilistic approaches is the opposite of scenario development approaches, lack of data and uncertainty provide a decision-maker with a narrow, often misleading answer, while scenario development methods can provide too broad a set of potential outcomes to be useful. Scenario planning avoids having to address uncertainty while probabilistic methods can quantify uncertainty.

In a typical process in nuclear security, the results of an intelligence assessment are provided in the form of a threat assessment, which documents a range of potential threats along with their objectives and capabilities. This is typically the only connection between the intelligence organizations and the nuclear regulatory authority, until the next time the threat assessment is updated.

The threat assessment is used to develop a design basis threat (DBT), which is a subset of the potential threats evaluated, and used as the basis for regulations to protect nuclear material, facilities, and activities, and used as the basis for the development of baseline scenarios to evaluate physical protection systems. Prioritizing the scenarios helps focus efforts and regulations on the most effective protection measures. Problems with estimating the probability of occurrence of different threats to prioritize them has proven to be too difficult a problem to solve. Other methods have been developed to avoid these issues, such as the Risk-Informed Management of Enterprise Security (RIMES), which compares security risks by comparing attack scenarios' levels of difficulty and consequences [12, 13].

In any event, once a baseline set of scenarios has been developed, vulnerability analyses are conducted to evaluate whether the defined threats possess the required capabilities to successfully complete an attack, assessments of the effectiveness of the protection of targets to different attack scenarios, and assessments of consequences of different types of attacks on different targets.

PROPOSED APPROACH

In the proposed approach, the current process is maintained, but the results of the vulnerability analysis are shared with the intelligence community responsible for conducting the threat assessment, and the results are combined detailed assessments of the planning stages required by defined threats to prepare for such an attack. This accomplishes two objectives: it improves future threat assessments, and it allows for the development of question sets regarding potential indicators of increased likelihood of an attack, similar to the questions in a PRA used to answer the question how likely it is to happen, but threat specific [15].

How likely is it to happen is associated with data necessary to collect to estimate the likelihood associated with a threat. An example of a range of estimates to express uncertainties in the data is defined in an intelligence community document [14]. The process involves determining what questions would need to be answered to estimate the likelihood of a threat in one of the following categories:

- Almost no chance
- Very unlikely
- Unlikely
- Roughly even chance
- Likely
- Very likely
- Almost certain

The question sets can then be used at nuclear sites to look for patterns in the physical world and in the cyber world that may indicate the possibility of a potential threat gathering intelligence to plan an attack. The specific nature of the questions can also be used by the intelligence community to identify patterns in the analyses they perform that may indicate an increased likelihood of attack. As determined in the Bien Hoa Air Base attack, a base with minimal protection, it was still complex enough to require careful and precise planning, including significant and prolong efforts to gather intelligence prior to the attack.

The intent of this effort is to strengthen the effectiveness of the regulatory framework by expanding regulations beyond simply requiring passive defensive measures and waiting for a threat to materialize, but by the addition of regulations to formally establish processes to work closely with the intelligence community to develop question sets used to link potential threats to clear, observable, and diverse patterns of behavior indicating an increased likelihood of attack. In addition, the regulatory framework can establish requirements to implement active security measures to augment protective measures for nuclear material, facilities, and activities. These measures are intended to put processes in place to look for indicators as defined in the question sets.

CONCLUSIONS

Regulatory development is based on a forecast of what the threats are, what their capabilities are, what their intent is, and what measures will provide adequate protection against them. To improve the regulatory framework, this proposal outlines a process to better use the resources of the intelligence community with the responsibility of conducting threat assessments that form the basis of protection regulations. It incorporates some of the applicable elements of the PRA process to implement a framework intended to augment passive, defensive physical protection elements with active security measures. The objective of implementing active security measures is to deter, disrupt, and detect potential threats by using intelligence driven question sets to identify patterns of behavior indicative of a potential threat to prevent an attack before it occurs, and not rely solely on the ability of the physical protection system to successfully defend an attack.

REFERENCES

[1] Mao Tse-tung, On Guerrilla Warfare, translated by Samuel B. Griffith III, Urbana: University of Illinois Press (2000).

[2] Douhet, G., The command of the air, translated by Ferrari, D., Washington, DC: Air Force History and Museums Program (1998).

[3] Fox, Roger, Air Base Defense in the Republic of Vietnam 1961-1973, Office of Air Force History, United States Air Force, Washington, DC (1979).

[4] Stephans, Richard A., System Safety for the 21st Century: The Updated and Revised Edition of System Safety 2000, John Wiley & Sons, Inc., New York (2004).

[5] U.S. Nuclear Regulatory Commission, WASH-1400 Reactor Safety Study: An Assessment of Accidental Risks in U.S. Commercial Nuclear Power Plants, NUREG-75/014, U.S. Government Printing Office, Washington DC (1975).

[6] Kaplan S., Garrick, B. J., On the Quantitative Definition of Risk, Risk Analysis, 1:1, (1981).

[7] Murphey, W.M., et al., Societal Risk Approach to Safeguards Design and Evaluation, ERDA-7, Energy Research and Development Administration, Washington DC (1975).

[8] Rasmussen N, N., Probabilistic Risk Analysis – Its Possible Use in Safeguards Problems, Proc. 17th Annual Meeting of the Institute of Nuclear Materials Management, Deerfield IL (1976).

[9] Richardson, J.M., Comprehensive Safeguards Evaluation Methods and Societal Risk Analysis, SAND82-0366, Sandia National Laboratories, Albuquerque NM (1982).

[10] Cox, Jr., L.A., Some Limitations of Risk = Threat × Vulnerability × Consequence for Risk Analysis of Terrorist Attacks, Risk Analysis, 28 No.6 (2008).

[11] National Research Council, Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex: (Abbreviated Version), Washington, DC: The National Academies Press (2011).

[12] Duran, F.A., et al, Risk-Informed Management of Enterprise Security: Methodology and Applications for Nuclear Facilities, SAND2013-7011C, Sandia National Laboratories, Albuquerque, NM (2013).

[13] Wyss, G.D., et al, A Method for Risk-Informed Management of Enterprise Security (RIMES), SAND2013-9218P, Sandia National Laboratories, Albuquerque, NM (2013).

[14] Office of the Director of National Intelligence, Analytic Standards, Intelligence Community Directive 203, Washington DC (2015).

[15] Willis, H. H., Using Risk Analysis to Inform Intelligence Analysis, WR-464-ISE, RAND Corporation, Santa Monica, CA (2007)