SAND2015-9504C

Exceptional service in the national interest

Sandia National Laboratories

Adversary Threat Environment and its Impact on Nuclear Security

Synopsis

"We can expect to see more of these cases, as long as the smugglers think they can make big money without getting caught, they will keep doing it."

-Constantin Malic, Moldovan Police Detective

AUTHORS:

Matthew Thompson
Sandia National Laboratories

David Ek
Sandia National Laboratories

John Pelletier
Sandia National Laboratories

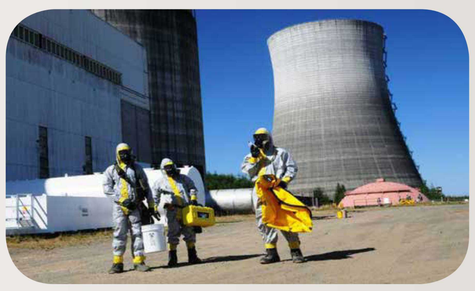
Fundamentals

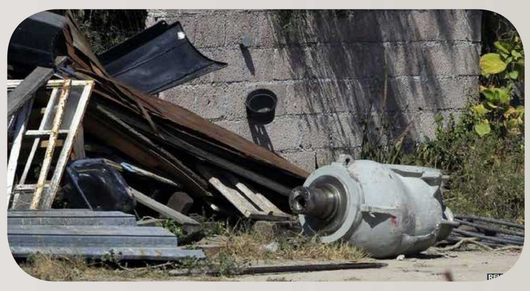
Security systems are intended to prevent the success of intentional, malicious acts that would result in unacceptable consequences. To prevent such intentional acts, some insight into the specific types of acts and the people who might perpetrate these acts is required. The security community refers to those who might undertake intentional, malicious acts as "adversaries" or "threats." Therefore, an understanding of the threats is fundamental to establishing the proper confidence level that a security system provides adequate protection.

Unfortunately, the threat environment is dynamic: the threats of today are vastly different to those of 10 years ago. Adversaries are increasingly more sophisticated, more dedicated, and more prevalent. This implies that the security systems used to defeat these threats must be increasingly more robust to successfully offset this increased threat.

Data

Open-source threat data was analyzed for significant terrorist and criminal acts in Europe over the past 5 years. The analysis focused on intentional, malicious acts involving nuclear and/or radioactive materials as well as acts involving theft and sabotage of high value targets, including banks, jewelry heists, and other targets with sophisticated security systems. In addition, events (realized or just planned) of sabotage against utilities, chemical factories, and other significant targets and those involving insiders, both acting alone and in collusion with outsiders were reviewed. The data collected was organized in a manner similar to a threat assessment.





Threat Criteria

The Amended Convention on Physical Protection of Nuclear Material and Nuclear Facilities outlines a set of Fundamental Principles of Security, one of which is the Principle of Threat. This principle indicates that a State's physical protection should be based on the State's current evaluation of the threat. Although the open-source threat assessment (TA) data that was gathered is reliable and relevant to the nuclear/radiological targets, it is not in a form that can be used to inform the design or evaluation of a security system. There are several reasons for this:

- First, a security system can be tailored to successfully detect, delay, and respond to specific adversary characteristics; however, conflicting characteristics of many adversary groups, such as is found in a TA, do not lend themselves to selection of specific design criteria. Clear adversary criteria with distinct characteristics are needed to facilitate appropriate system design. Left with a multitude of diverse adversary characteristics, the security system designer is forced to assume (explicitly or implicitly) characteristics of a randomly imagined composite adversary, drawn from the diverse adversary groups in the TA.;
- Second, threats are dynamic but security systems are static. A security system might have a 10- to 20 year lifetime, whereas threats can evolve as quickly as a few months. To address this, the threat criteria needs to be forward looking and conservative, while staying within the realm of credibility and the bounds of fiscal reality.

The process to develop appropriate threat criteria from a TA is described in Nuclear Security Series #10. These steps are:

1. Screen the threat assessment to ensure that all threats are relevant for a nuclear security threat criteria;
2. Merge the characteristics of the various adversary groups into a credible and representative composite adversary description; and
3. Modify the composite adversary characteristics based upon policy considerations.

The resulting threat criteria will more closely represent the actual level of threat observed in the TA, while also reflecting the relevant policy considerations. This could then be used by the regulatory authority to dictate performance-based requirements for the design and operation of the nuclear security systems at licensees. By so doing, confidence is gained that the nuclear security regime is effectively protecting the public from potential adverse consequences that could result from the peaceful use of nuclear and radioactive materials.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. | SAND2015-XXXX X

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration