SAND2019-14573C

DEVELOPMENT OF A FRAMEWORK FOR ANALYZING IMPACT OF EMERGING TECHNOLOGIES ON NUCLEAR AND RADIOLOGICAL SECURITY

A.A. SOLODOV
Sandia National Laboratories[1]
Albuquerque, NM, USA
Email: aasolod@sandia.gov

C. POTTER, S. HOROWITZ, J. LIEBERMAN, L. GILBERT
Sandia National Laboratories
Albuquerque, NM, USA

Abstract

Rapid advancement in technological development has a profound effect on the world around us. In this context, the influences that these advances could have on the nuclear and radiological security are changing rapidly and dramatically. Nuclear operators and security stakeholders are already investing significant resources to address some of these new emerging threats and integrate new technological solutions into security systems. However, systematic understanding of this massive technology evolution is of vital importance to follow the trends and identify both potential vulnerabilities and opportunities to increase effectiveness and prioritize investment areas. The study was designed to enable decision makers to evaluate the potential impact of emerging technologies and the way those technologies are implemented on nuclear and radiological security, now and into the future. The main objective was to develop an understanding of these: How might emerging technologies both create and address future risks to securing nuclear and radiological materials around the world? The paper describes the analysis framework that was developed by Sandia to perform a systematic analysis of a large number of emerging technologies and prioritizing them with regards to their impact on the field of nuclear and radiological security. Several examples of analysis and outcomes are also shown.

1. INTRODUCTION

A systematic understanding of the present massive technological evolution is critical in order to anticipate and timely address emerging threats and opportunities presented by the prevalence of new technologies. Additionally, there has been a structural shift in technology development and innovation in recent decades. In the past, government funded research drove technological development and advancement, while private industry played a smaller role of integrating government innovations into commercial products. This situation has changed, and now private sector companies appear to be the main engines behind technological development with the governments playing a catch-up role in many areas. As the pace of technological development increases and government development slows, it is increasingly urgent that government agencies responsible for nuclear and radiological security have a systematic and thorough understanding of the current technological landscape. Analysing the trends and effects of emerging technologies present an opportunity to increase understanding of both vulnerabilities and opportunities, and to prioritize investment areas.

2. ANALYSIS FRAMEWORK

The central task of this work was to create an effective analysis framework that would be capable of bringing together a large number of technologies, assessing their impact on the field of nuclear and radiological security, and prioritizing them. A number of requirements were established for the framework. Those are to:

---

[1] *Sandia National Laboratories is a multimission laboratory operated by National Technology and 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. Sandia Labs has major research and development responsibilities in nuclear deterrence, global security, defense, energy technologies and economic competitiveness, with main facilities in Albuquerque, New Mexico, and Livermore, California. SAND2019-XXXX*

– effectively address specific mission areas related to nuclear and radiological security
– be robust (capable of handling a large number of technologies and applications)
– be scalable (capable of adding and removing technologies to the analysis)
– be flexible (capable of producing results for specific, more narrow mission areas).

2.1. Structure of the Analytical Framework

The analytical framework was developed in a form of a matrix with technologies and applications in rows and criteria defining the nuclear and radiological security mission areas in columns. The intersecting squares contain potential scenarios and scores assigned to them. This structure allows for the analysis of technologies against various criteria and the grading of each technology's contribution to various functional areas. The schematics of the analysis structure are shown in Figure 1.

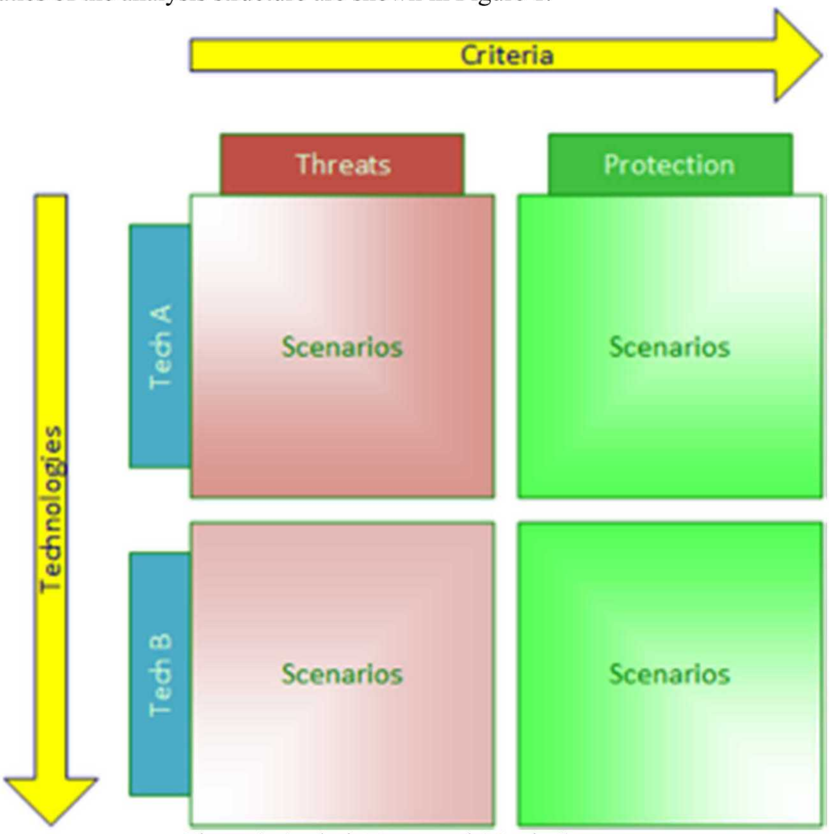

Figure 1. Analysis Framework Matrix Structure

The analysis performed for the purpose of our study consisted of several distinct steps. During the first stage, a list of technological concepts and applications was compiled through literature search and interviews of technology and security experts. The intention was to create as comprehensive a list as possible within limitations of time and resources available. Analysis criteria were developed in conjunction with the assembly of a technology list. Two categories of criteria were developed: threat and protection. The main requirement for analysis criteria were for each one to address a specific functional area within nuclear and radiological security mission. All criteria were weighted for further comparison.

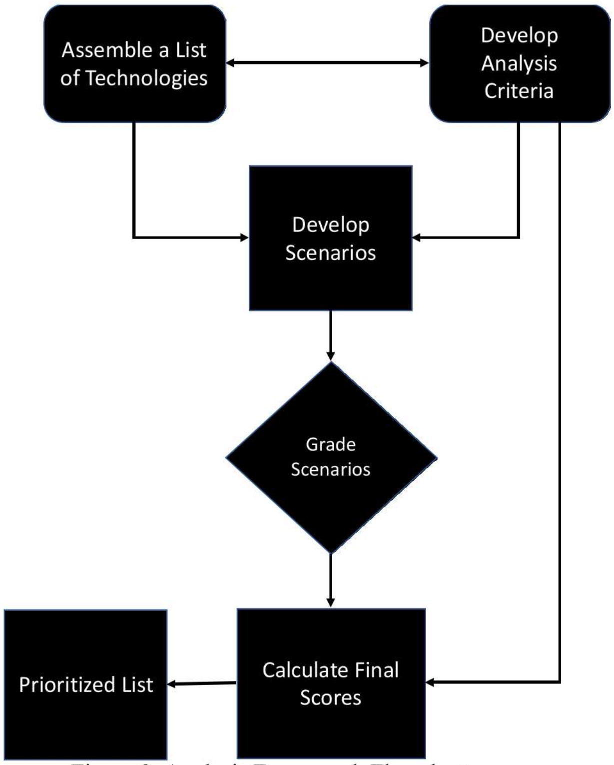

Figure 2. Analysis Framework Flowchart

In the following steps of analysis, specific scenarios for each technology-criteria pair were developed, scenarios were graded using risk matrices, and final scores for each technology were calculated. Based on the final scores, the prioritized list of technologies was assembled. The analysis framework flowchart is shown in Figure 2.

2.1.1. Criteria and Weighting

Two sets of criteria were developed: threat criteria and protection criteria. A total of thirteen criteria were used in the analysis. Some examples of threat criteria included sabotage, theft, knowledge and expertise transfer, etc. Examples of protection criteria included training, deterrence, and sustainability. All criteria were weighted by subject-matter experts (SMEs) through the use of a questionnaire. Weights were used to integrate scoring of individual scenarios into overall technologies and applications scores. The responses collected from all participants were averaged to obtain single weight for each individual criterion to be used in the analysis.

2.1.2. Scenarios

Once the list of technologies and the criteria set were finalized, the next step was to develop scenarios for each square within the matrix. The scenarios described how specific technologies may impact the functional area encompassed by criteria relevant to nuclear and radiological security. Due to the large number of technologies investigated in this study, it was necessary to develop scenarios that were concise (one to two sentences) but at the same time meaningful and descriptive. This approach allowed for the analysis of an extensive set of technologies in a reasonable amount of time, producing meaningful analytical results.

Scenarios were developed by a group of SMEs during the course of specially facilitated workshops. Prior to conducting a workshop, draft scenarios were developed by individual SMEs. During the workshops, all scenarios were reviewed and modified until consensus was reached among the SMEs.

2.1.3. Risk Matrices

In order to quantify a scenario's impact and develop a numerical evaluation of the technologies and applications, a set of risk matrices was used. Their purpose was to allow SMEs to qualitatively grade the likelihood of a particular scenario taking place in the future. The risk matrices also allowed the SMEs to assess the impact that a scenario would have on nuclear and radiological security. The matrices had four degrees of likelihood ranging from *improbable* to *highly probable* while impact had four degrees of consequences ranging from *acceptable* to *intolerable* for threats and from *trivial* to *critical* for protection. Once the likelihood and impact were assessed, a score from the matrix was assigned to each scenario. The risk matrices used in this study are shown in Figure 3. Scenario grading was done during a special workshop in which consensus was reached within the group of SMEs. At first, each SME independently would assign scores to a scenario, then the scores were compared and discussed. Finally, a consensus was formed through discussion and a final score assigned for a given scenario.

Threat

	IMPACT			
	A	T	U	I
	ACCEPTABLE LITTLE TO NO EFFECT ON THE SYSTEM	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL	UNDESIRABLE SERIOUS IMPACT TO THE SYSTEM MISSION	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE UNLIKELY TO OCCUR	LOW – 1 –	LOW – 2 –	MEDIUM – 6 –	HIGH – 9 –
POSSIBLE MAY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 10 –
PROBABLE WILL MOST LIKELY OCCUR	MEDIUM – 6 –	HIGH – 8 –	HIGH – 9 –	EXTREME – 11 –
HIGHLY PROBABLE WILL DEFINITELY OCCUR	HIGH – 8 –	EXTREME – 10 –	EXTREME – 11 –	EXTREME – 12 –

Protection

	IMPACT			
	TRIVIAL LITTLE TO NO EFFECT	MINOR EFFECTS ARE FELT, BUT NOT CRITICAL TO THE MISSION	MAJOR SERIOUS IMPACT ON THE MISSION	CRITICAL COULD RESULT IN A COMPLETE CHANGE OF APPROACH
LIKELIHOOD				
IMPROBABLE UNLIKELY TO OCCUR	LOW – 1 –	LOW – 2 –	MEDIUM – 6 –	HIGH – 9 –
POSSIBLE MAY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 10 –
PROBABLE WILL MOST LIKELY OCCUR	MEDIUM – 6 –	HIGH – 8–	HIGH – 9 –	EXTREME – 11 –
HIGHLY PROBABLE WILL DEFINITELY OCCUR	HIGH – 8 –	EXTREME – 10 –	EXTREME – 11 –	EXTREME – 12 –

Figure 3. Risk matrices for threat and protection analysis[2].

2.1.4. Final Technology Scores

Once the scenarios were complete and graded, final technology scores were calculated. Scenario grades and criteria weights were used to perform the calculation, where the following equations were used:

$$TTS_i = \sum_{j=1}^{N} t_j \cdot X_j$$

[2] Risk matrices adapted from a template available at https://www.smartsheet.com/all-risk-assessment-matrix-templates-you-need

where:
TTS_i – technology i threat score
t_j – threat criteria j weight
X_j – threat scenario j score

$$TPS_i = \sum_{j=1}^{M} p_j \cdot Y_j$$

where:
TPS_i – technology i protection score
p_j – protection criteria j weight
Y_j – protection scenario j score

2.1.5. Technology Prioritization

The last step of the analysis was assembling the final prioritized list of technologies and applications. Because the analysis was based on two categories of criteria and separate scores for threat and protection, the final results were presented in a form a two-dimensional plot. The threat score was plotted along the abcissa and protection score along the ordinate.

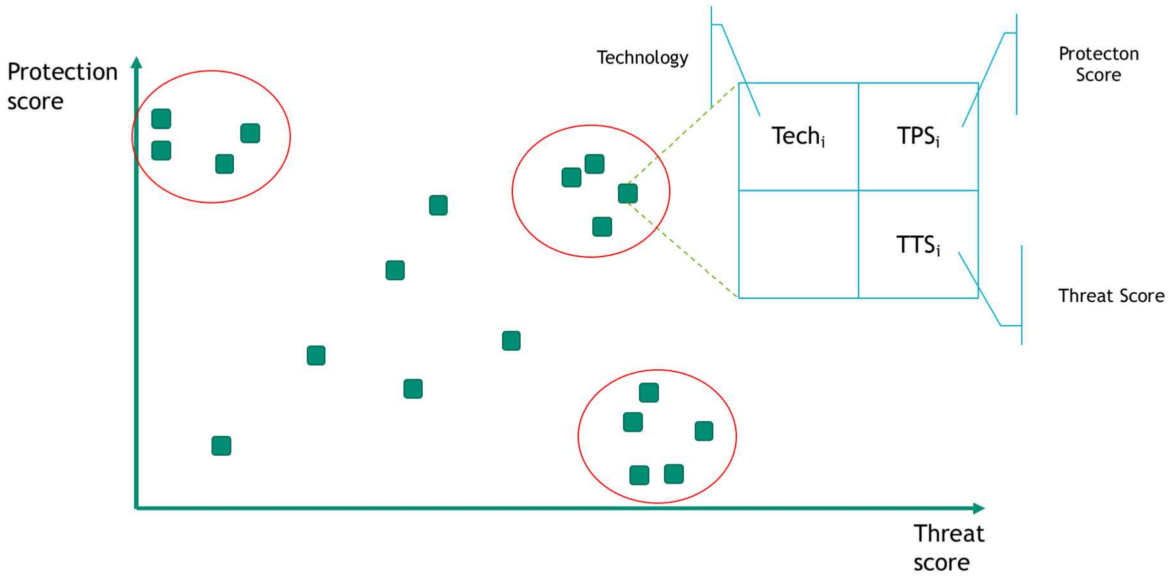

Figure 4. Final Analysis Output Graph

3. SAMPLE ANALYSIS

What follows is a short demonstration of applying this framework to an analysis of emerging technologies as they impact nuclear and radiological security. This sample is only intended to show how the analysis works and the results are not intended to be used in any type of decision-making.

3.2. List of Technologies

In the analysis described here, the distinction between *technological concept* and *technological application* is made. Broad technological concepts such as artificial intelligence (AI) serve as high level categories for specific technological areas. Technological applications as defined here are specific technologies or tools created for a particular task using the emerging technological concepts. An example of a technological application would be *predictive policing* using AI.

Three technological concepts will be used here to demonstrate the analysis process and outcomes. Within these technological concepts five specific applications were selected as outlined and defined in TABLE 1.

TABLE 1. List of technologies used in sample analysis.

Technology Application	Definition
Additive Manufacturing	Additive manufacturing is the official industry standard term (ASTM F2792) for all applications of the technology defined as the process of joining materials to make objects from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies.
low volume production	Capability to produce unique and complex design items or parts in single items; no production line needed
counterfeit goods production	Goods or components designed and produced to mimic a trusted product from a trusted supplier
Artificial Intelligence	The theory and development of computer systems able to perform tasks that normally require human intelligence such as visual perception, speech recognition, decision-making, and translation between languages.
predictive policing	Using AI to predict and prevent crime
Autonomy	Capability of machines to operate and perform tasks independently without explicit human control.
assured autonomy	An autonomous system's ability to accomplish goals independently or with minimal supervision from human operators in environments that are complex and unpredictable.
autonomous weapons	Lethal devices that have been empowered by their human creators to survey their surroundings, identify potential enemy targets, and independently choose to attack those targets on the basis of sophisticated algorithms.

3.3. Analysis Criteria

The next step after selecting technologies was in specifying analysis criteria. Again, for simplicity of demonstration, a total of five criteria were chosen, two of them in the *threat* category and three in *protection* category. Simple weights were assigned to criteria for demonstration. The full list of criteria with definitions and weights is shown in TABLE 2.

3.4. Scenarios and Analysis

The next step was development of scenarios for technology/criteria pairs and grading these scenarios using risk matrices shown in Figure 3. For a large number of technologies and criteria it may be extremely labour intensive to develop detailed intricate scenarios; therefore, the approach suggested is to create brief but meaningful scenarios for each technology-criteria pair. Several examples of scenarios for the technologies and criteria used are shown below.

1. *Counterfeit goods production/Sabotage*: Building counterfeit parts designed to fail to be supplied to a facility to be sabotaged
2. *Predictive policing/PP*S: Predictive policing would extend the PPS further outside of facility boundaries through early identification of potential threats & adversaries
3. *Assured autonomy/Theft*: Fully autonomous vehicles may aid in theft of nuclear/radiological materials by providing get away vehicles. This could also reduce the number of human attackers needed, and additional vehicles could be used as a decoy.
4. *Autonomous weapons/Theft*: Autonomous weapons may be used to distract response forces or lower a response force's probability of neutralization by providing additional fire power for the adversaries. This eliminates tasks that must be completed by a human and makes smaller design-basis threats more effective, as they are able to engage multiple targets using what are essentially tools.
5. *Autonomous weapons/Deterrence*: Autonomous weapons may serve as a strong deterrence against attacks on a facility.

TABLE 2. List of criteria used in sample analysis

Criteria	Definition	Weight
	Threat	
Theft	Theft of nuclear or radiological materials with the purpose of constructing an improvised nuclear device, radiological dispersal device, or radiological exposure device by a non-state actor.	0.4
Sabotage	Any deliberate act directed against a nuclear or radiological facility or nuclear/radiological material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances	0.6
	Protection	
Physical Protection System (PPS)	Integration of persons, procedures, policies, and detection/delay/response infrastructure which attempts to mitigate the risk of unauthorized removal of nuclear or radiological material, the sabotage of material or systems which could lead to radiological consequences, or other malevolent human acts.	0.5
Training	Cooperative interactive activity which contributes to the development of persons, procedures, guidelines, policies, techniques, infrastructure, and culture through the use of educational curricula, exercises, tabletops, workshops, meetings, conferences, discussions, or other cooperative educational activities which enable and enhance the trainee's capacity to secure nuclear and radiological materials and protect against their smuggling and/or malicious use.	0.3
Deterrence	Technologies that discourage the adversary from performing acts of radiological or nuclear terrorism, theft, or smuggling. These technologies could increase the difficulty of the operation itself, increase the probability of interdiction before the operation can be completed, or increase the probability of the perpetrator being identified after completion of the operation (forensics).	0.2

To demonstrate the approach to scoring, scenarios 1 and 5 were picked and graded. Using risk matrices shown in Figure 3, the likelihood and potential consequences of these scenarios were evaluated. For scenario 1, the likelihood of technological development for additive manufacturing to reach the level that would provide an adversary a capability to create counterfeit parts designed to fail and be supplied to a targeted facility was selected as *highly probable*. The impact of such scenario could reach an *undesirable level*. Therefore, based on the threat risk matrix the overall score for this scenario was 11.

For scenario 5, the likelihood of autonomous weapons being implemented in a PPS of a nuclear facility is low due to the ongoing debate about trust in such systems and ethical issues surrounding them; therefore, it was graded as *improbable*. The impact of such systems implemented on PPS deterrence would be *major*. Based on this assessment, a score of 6 was assigned to this scenario using protection risk matrix.

An example analysis with calculated final scores for each technology using scenario scores and criteria weights are shown in

TABLE 3 and TABLE 4.

TABLE 3. Sample analysis for threat

Technology\Criteria	Theft	Sabotage	Total
Additive Manufacturing			
low volume production	8	2	**4.4**
counterfeit goods	5	11	**8.6**
Artificial Intelligence			
predictive policing	8	8	**8**
Autonomy			
assured autonomy	10	11	**10.6**
autonomous weapons	12	12	**12**

TABLE 4. Sample analysis for protection

Technology/application	PPS	Training	Deterrence	Total
Additive Manufacturing				
low volume production	8	6	2	**6.2**
counterfeit goods	0	2	0	**0.6**
Artificial Intelligence				
predictive policing	12	8	9	**10.2**
Autonomy				
assured autonomy	12	11	9	**11.1**
autonomous weapons	10	5	6	**7.7**

Once the final scores were calculated, the results were plotted on a two-dimensional plot as shown in Figure 5. From the graph, the relative impact of technologies on threat and protection categories can be assessed and prioritized list of technologies can be created.

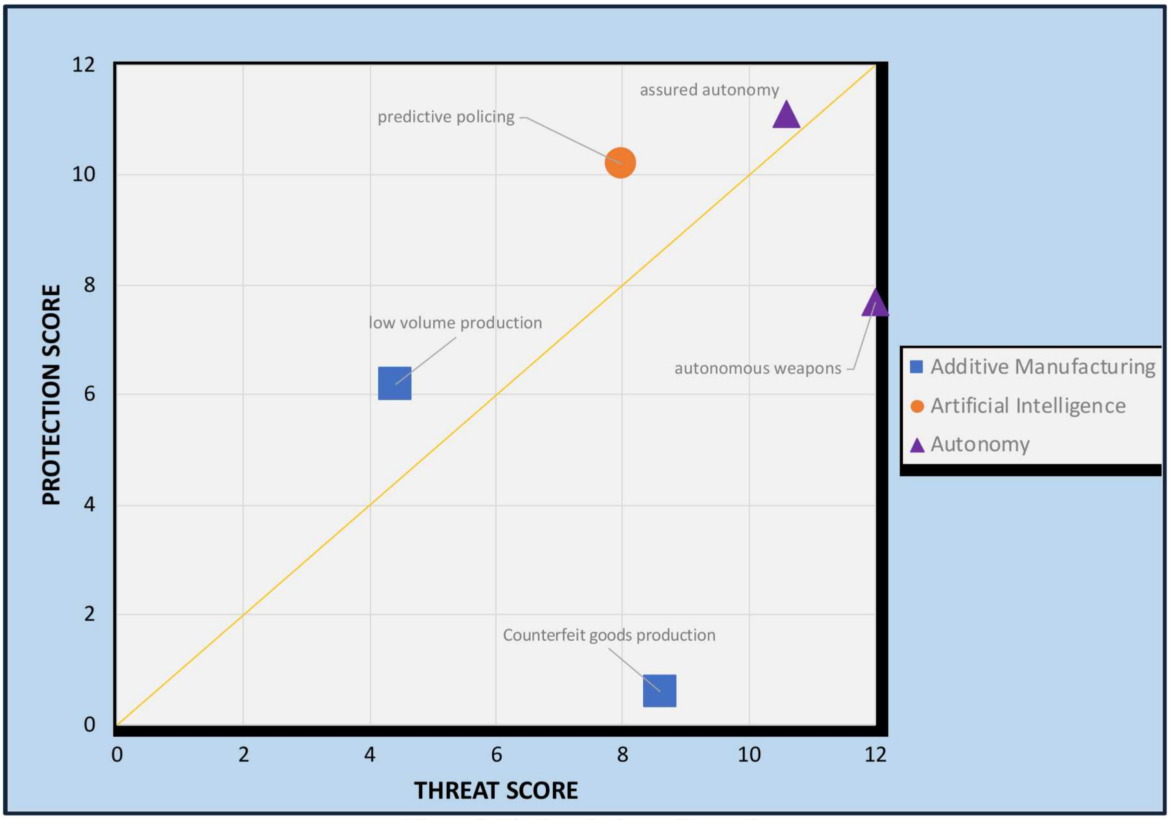

Figure 5. Final analysis results graph

4. CONCLUSIONS

Emerging technologies can have a profound impact the field of national security and, in particular, nuclear and radiological security and detection of materials outside of regulatory control. Acknowledging the importance of having a thorough understanding of the technological world, Sandia has developed an analysis methodology that allows for assessment and prioritization of the impact of new technologies. Within this framework, analysis is performed in a series of steps starting with development of a set of criteria, followed by collecting a list of technologies, and finally developing scenarios for each technology-criteria pair and grading these scenarios. The outcome is a set of prioritized lists based on the potential threats and benefits technologies can bring to the nuclear and radiological security.

The analysis framework developed allows for the comparison of multiple technologies and their effects and prioritization through quantitative analysis. While being quantitative, the analysis process relies heavily on SMEs' opinion, adding a degree of subjectivity to the results. The effects of subjectivity can be mitigated by increasing the number of SMEs as well as by diversifying the SME group's areas of expertise.

ACKNOWLEDGEMENTS

Authors would like to express their gratitude to the Office of Global Material Security of the National Nuclear Security Administration of the U.S. Department of Energy for financial support of this work.