International Journal of Nuclear Security

Volume 7
Number 2 *Special Issue for Women in Nuclear Security*
Article 7

1-2022

A Game Theoretical Model of Radiological Terrorism Defense

Shraddha Rane
Purdue University

Jason Timothy Harris
Purdue University - Main Campus

International Journal of Nuclear Security, Vol.7, No.2, 2022 – SPECIAL ISSUE FOR WOMEN IN NUCLEAR SECURITY

A Game Theoretical Model of Radiological Terrorism Defense

Shraddha Rane and Jason Harris
Purdue University

Abstract

Radiological dispersal devices (RDD) pose a threat to the United States. Healthcare facilities housing high-risk radioactive materials and devices are potentially easy targets for unauthorized access and are vulnerable to malevolent acts of theft or sabotage. The three most attractive candidates for use in RDD considered in this study are: ^{60}Co (radiosurgery devices), ^{137}Cs (blood irradiators) and ^{192}Ir (brachytherapy high dose radiation device). The threat posed by RDDs has led to evaluating the security risk of radioactive materials and defending against attacks. The concepts of risk analysis used in conjunction with game theory lay the foundations of quantitative security risk management. This paper develops a two player non-cooperative one-shot simultaneous defender-attacker game. The defender (healthcare facility) chooses to defend one of the three high-risk radioactive material targets and the attacker (terrorists or adversaries) chooses to attack one of the three high-risk radioactive material targets. A risk-informed approach is used to model players' payoffs or expected utilities for each choice of strategies. A game-theoretic model (RDD game) captures the strategic interaction between competing players who act rationally to maximize their expected utility. The evaluation of the RDD game results in a von Neuman max-min strategy solution being preferable to a mixed strategy Nash equilibrium solution. The von Neumann max-min strategy solution of the defender defending cobalt and the attacker attacking cesium is found to be the most prescriptive result, thus favoring the current efforts of phasing out cesium blood irradiators and replacing them with alternative technologies. The RDD game not only gives the defender strategic options to budget scarce security resources but also helps healthcare facilities make optimal choices under severe uncertainty about the terrorist threat.

Keywords: game theory, RDD, radiological terrorism, utilities, attacker-defender, max-min.

I. Introduction

The global economy has several critical infrastructure sectors with political and national security importance that are potentially vulnerable to deliberate attacks by terrorists and other motivated adversaries. Considering the strategic nature of the attacker, protecting such structures against intentional

doi:10.7290/ijns07vrqk

attacks is fundamentally different from a random accident or acts of nature. Healthcare facilities and university campuses are examples of infrastructures that face an increase of perceived security threats stemming from radiological terrorism. Healthcare facilities around the world that routinely use radioactive materials to diagnose and treat illnesses are well-trafficked and purposely open to the public, making them highly susceptible to a terrorist attack. Radiological terrorism, including the use of a radiological dispersal device (RDD) or radiological exposure device (RED), are among the most likely weapon scenarios because of their relatively simple technology and widespread use of radioactive material. Therefore, it is imperative for the healthcare sector to use the principles of graded and risk-informed approach toward building the defenses for source security.

The classical risk assessment approach takes the perspective of a single entity (industry, individual, defender) in identifying the threats that could negatively impact its ability to conduct business. The elements of game theory, on the contrary, assumes a rational opponent and evaluates the incentives and actions of both the entities (defender and attacker) affecting each other, with a goal of maximizing their own individual outcome. Rajbhandari & Snekkenes **[*1*]** and Cox, Jr **[*2*]** provide an articulate and a detailed comparison of how game theory fits into and aids the risk assessment process to effectively manage threats from adversaries. This paper demonstrates the mapping between the two approaches by adapting the specific steps of risk assessment outlined in the precursor parts of this work **[*3*]** and applying it to the game theoretic model workflow. The main contribution of this paper is to show how game theoretic analysis could be an effective way to both defend against an attacker whose choice of target is unknown and selectively deploy security resources based on the current evaluation of threat.
To enable the readers to have a better understanding of both methods, we structured the remainder of the paper is as follows. In Sect. II, we present the quantitative model of the Potential Facility Risk Index (PFRI) and a summary of its mathematical framework. In Sect. III, we summarize the key game theory concepts, notations, assumptions, and mathematical formalism. Sect. IV provides a more detailed application of game characteristics and mapping between the two approaches. Conclusion and discussion of our findings are given in Sect. V.

II. The Potential Facility Risk Index (PFRI) - Background

The iterative process of risk-informed approach **[*4*]** forms the basis for the quantitative model of the Potential Facility Risk Index (PFRI). The PFRI can be defined as a mathematical framework that uses the triplet definition of risk by identifying the threat, evaluating the vulnerabilities, and calculating the resulting consequences, given the occurrence of the attack **[*3*]**. The PFRI, unique to the facility, can be used by radiological facilities to conduct self-assessments and gain a better understanding of the threat they face. Rane & Harris **[*3*]** formally introduces the novel PFRI framework by presenting and applying each element of risk to a hypothetical medical facility. Figure 1 presents the complete PFRI framework.

doi:10.7290/ijns07vrqk

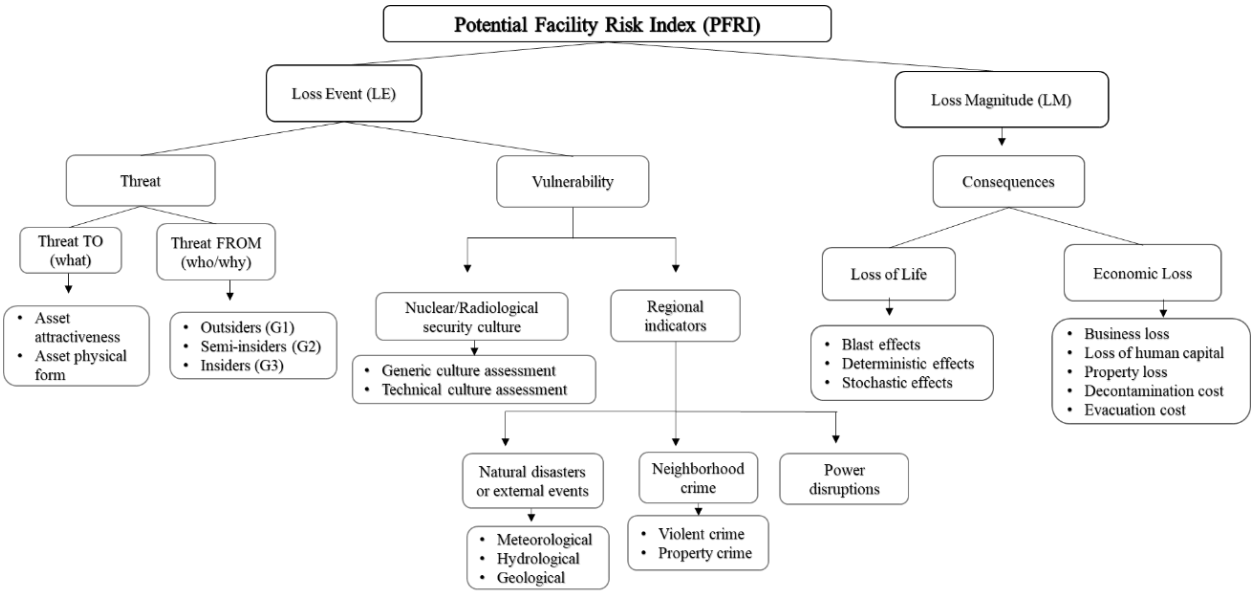

Figure 1. The complete PFRI framework [*3*]

The threat component of the PFRI model identifies threat as: (1) threat 'from'- adversaries who may attempt a malicious act, and (2) threat 'to'- radioactive or other nuclear material assets that the adversary might seek to harm. A multi-attribute utility function is used to solve for the asset preference and intentions of the threat adversaries. The material utility function $U[mat]$, mathematically presented as a product of $U[attractiveness]$ and $U[form]$, integrates the attributes of the relative attractiveness of radiological material based on the International Atomic Energy Agency (IAEA) categorization system and the physical from (metallic, powder, etc.) of the radionuclide Eq (1) to (3).

$$U[mat] = U_i[attractiveness] \times U_i[form] \quad (1)$$

$$U_i[attractiveness] = 1 - e^{\left(-\left[\frac{\frac{A}{D}}{m_r}\right]^3\right)} \quad (2)$$

$$U_i[form] = 1 - e^{(-[F_r]^3)} \quad (3)$$

where i is the index of the radionuclide (weapon chosen as a dispersal device);
A is activity of the radionuclide in TBq;
D is the danger value of the radionuclide in TBq;
m_r is the mass of the radionuclide in kg; and
F_r is the physical form index of the radionuclide (metallic = 1, powdered salt = 2)

The adversary utility, U[adv], assesses the adversarial mindset of the attacker as a measure of symbolism or intent, X_SY, casualties or life loss, X_LL, from the attack, and the degree of economic damage, X_ED, from the attack. Swing weights, quantified on a scale of 0 to 1, are used to rank the attributes, X_k, based on the analyst's perspective of the adversaries' value tradeoffs. Once a complete set of fundamental objectives or motivations is identified, the multi-attribute utility function is linearly additive **[*5*]**.

$$U(X_k) = sqrt(X_k),\ k = 0\ to\ 2 \quad (4)$$

$$U[adv] = \sum w_k U(X_k), k = 0\ to\ 2 \quad (5)$$

where k is the index of different attack attributes;
w_{jk} is the value tradeoff in the form of swing weights;
$u(X_k)_j$ is the value function of attribute k for threat group j; and

doi:10.7290/ijns07vrqk

$U[adv]$ is the adversary utility function.

The total utility function, *U[tot]*, equals the product of the material input, *U[mat]*, and adversary's utility function, *U[adv]*.

To further the profiling of the threat event, observers develop a set of plausible attack scenarios, evaluating each asset separately. To realistically represent the malicious intent of theft or sabotage, observers make assumptions on the following parameters: the physical protection system, adversary capabilities, probability of detection, number of entry and exit points, and adversary task times. The probability of interruption, P_I, is computed using the Estimate of Adversary Sequence Interruption (EASI) tool **[*6*]**. The components of Probabilistic Risk Assessment (PRA) supplement the pathway analysis, delineating various initiating events (i.e., an undesired event challenging the facility security) that if taken advantage of by an opportunistic adversary may result in a theft or sabotage. Depending on the asset and the asset specific scenarios, scheduled maintenance days, radiation device repair days, source replacement durations, security feature failures and other equipment unavailability times are identified as initiating events. With respect to the PRA parameters of the incident frequency, number of trials and the rate of occurrence, the probability model of binomial, Poisson and normal distribution functions is applied accordingly to estimate the overall success probability of theft, P_s. The adversary in the PFRI framework, assumed to be rational and intelligent, evaluates all attack scenarios known to them and chooses the scenario that maximizes their expected utility. The expected utility of each attack scenario is computed as the product of the overall success probability of theft and the total utility function of the adversary **[*3*]**.

To evaluate the consequences, the PFRI framework assumes that the theft of the radioactive material was successful. The consequences of the radiological dispersal device (RDD) are examined as a function of: (1) loss of life, C_{LL},, resulting from immediate fatalities from the blast, acute radiation exposure, and stochastic effects caused by airborne dispersal of radioactive material, and (2) economic loss, C_{EL}, resulting from decontamination costs, evacuation costs, business losses, and property loss.

$$C_{LL} = -[\left(\frac{D_{BE}+D_{cancer}+D_{ARS}}{Population\ density}\right) + \left(\frac{I_{BE}}{Population\ density}\right)] \qquad (6)$$

C_{LL} is the life loss consequence severity variable
D_{BE} are the fatalities from the blast effects
D_{cancer} are the fatalities in future from relative cancer risk
D_{ARS} are the fatalities from Acute Radiation Syndrome (ARS); and
I_{BE} blast effect morbidity.
I_{cancer} is relative cancer risk morbidity; and
I_{ARS} is the deterministic effect morbidity

The economic consequence loss value, C_{EL},, represents the severity of the monetary loss directly or indirectly resulting from an executed RDD threat event.

$$C_{EL} = \sqrt{(I - D_E)^{-1}Y} \qquad (7)$$

C_{EL} Economic Loss (EL) consequence severity variable
D_E is the difference between the two vector components A_e and B_t ; and
Y is the linear regression coefficient.

$$A_e or\ B_t = \frac{E_{et}}{\sum E_t} \qquad (8)$$

doi:10.7290/ijns07vrqk

Coefficients denoted by B_t and $A_e$for before and after the RDD event, respectively, are obtained by dividing each economic variable entry (E_{et})by its corresponding column total ($\sum E_t$)Where, e, is the index of economic variables and t is the index of the states of the economy (i.e., before and after the RDD attack).

The net consequence loss (C_{net}) is calculated by taking the average of C_{EL} and C_{LL}.

$$C_{net} = \frac{(C_{EL}+C_{LL})}{2} \qquad (9)$$

A detailed description of the above parameters is provided in our previous work Rane & Harris **[*3*]**. A numeric score is allocated to each of the risk triplet of threat, vulnerability (discussion of which is omitted due to its inapplicability in this paper), and consequence to devise one composite number of the PFRI metric, unique to the facility Eq (10). The PFRI risk chart, quantified on a scale of 1-10, with a score of 1 meaning "very low risk" and a score of 10 meaning "very high risk", can be used to communicate risk effectively and succinctly to the public.

$$PFRI = e^{[\max(EU[X_{ij}])\times\left(V+\left(1-\min\left(Z_{gen},Z_{tech},Z_{sub}\right)\right)\right)\times C_{net}]} \qquad (10)$$

The background of the PFRI is prominently featured in the discussion of this paper is because it provides probabilities of a successful attack and consequences for pairs of attacker-defender strategies. Obtaining this information is often seen as the heart of the practical problem that defenders need solved **[*2*]**. The PFRI framework, including threat profiling, pathway analysis, PRA of how events may unfold during and following an attack, and consequence modeling of the results, is essential for developing a game-theoretic model.

III. Introduction and Basics of Game Theoretical Model

Game theory is an abstract mathematical theory for analyzing interactions among multiple decision makers, also known as players. Game-theoretic models are well suited to examine the possibility of achieving an optimum stable solution between the adversary and the defender. The decision makers may be nations, people, robots, or even corporations **[*7*]**. The preferences of each player are specified by utility functions, as described in Section II, that quantify the amount of benefit resulting to each player from possible outcomes of the game; this benefit is referred to as the payoff. A player's strategy in a game is a complete plan of action for whatever situation might arise. The strategy fully determines the player's behavior. Each player has two or more strategies or specific choices. Strategy profiles, which are the possible combinations of strategies that can be used by the players, give different payoffs to each player **[*7*]**. In this context of radiological source security, players are: (1) the defense forces of the healthcare facility on one side and (2) the terrorist or the attacker on the other side. This paper examines the strategic interaction between the two.

The work presented uses elements of non-cooperative game theory. Cooperative and non-cooperative theories are the two leading frameworks for analyzing games. Non-cooperative games are those in which the sets of possible actions of individual players give an outcome. Cooperative games are those in which the sets of possible joint actions of groups of players give an outcome. The players in a noncooperative game compete against each other, and each player is selfishly interested only in their own payoff. In some noncooperative games the players have perfect information about the game (such as chess), while in other cases, the players may have incomplete or asymmetrical information (such as many card games).

Equilibrium states are possible for one-shot games (games played only once), finitely repeated games, or infinitely repeated games. Nash equilibrium, named after Nobel laureate John Forbes Nash, is the most

doi:10.7290/ijns07vrqk

used solution concept in game theory. This notion captures a steady state play of a strategic game in which each player holds the correct expectation about the other player's behavior and acts rationally **[7, 8]**. If each player has chosen a strategy and neither player can increase their payoff by choosing an action different from his current one, then the current set of strategy choices and the corresponding payoffs constitute a Nash equilibrium.

In this paper, a simultaneous one-shot non-cooperative game is applied to a healthcare facility (defender or player 1) housing radiation emitting devices and radioactive sources. The healthcare facility is defending its assets against a terrorist RDD attack (attacker or player 2).

A. Notations and the Mathematical Formalism

For this study, we define the following sets and functions:

Players $i \in I = \{1,2\}$ where Player 1 is the healthcare facility, or the "defender" and Player 2 is the terrorist or the "attacker".

The study limits the asset (radioactive material) list to the highest value targets (i.e., high likelihood of success and high impact) available, rather than all the potential targets in the medical facility. Of the hundreds of radioactive materials available, the three generally found in healthcare facilities are considered the most attractive candidates for use in RDD: ^{60}Co (radiosurgery devices), ^{137}Cs (blood irradiators) and ^{192}Ir (brachytherapy HDR device). The sources threatened with attack are the set $k \in K = \{Co, Cs, Ir\}$ with Co being the atomic symbol for cobalt, Cs being the atomic symbol for cesium, and Ir being the atomic symbol for iridium.

Let S_i be the strategy space comprising each of the possible strategies $s_{ik} \in S_i$, where the k_{th} source is targeted by the i_{th} player. The strategy space of player 1 is $S_1 = \{defend\ Co, defend\ Cs, defend\ Ir\}$. The strategy space of player 2 is $S_2 = \{attack\ Co, attack\ Cs, attack\ Ir\}$. The pure strategy profile is a vector of the form $s = [s_{1k}, s_{2k}]$ that gives a particular combination of pure strategies that the players can choose. The Cartesian product $S_1 \times S_2$ is the set of all possible pure strategy profiles in the game[1].

A mixed strategy θ_i is a randomization over pure strategies. Let Θ_i denote the space of player i's mixed strategy probabilities, $\theta_i(s_{ik})$, where θ_i is the probability assigned to the player i for defending or attacking the k_{th} source such that for each player i, $\theta_i(s_{ik}) \in [0,1]$ and $\sum_{ik} \theta_i(s_{ik}) = 1$.

$\boldsymbol{\rho_{in}} = [\theta_i(s_{i,Co}), \theta_i(s_{i,Cs}), \theta_i(s_{i,Ir})]$, $\boldsymbol{\rho_{in}} \in \Theta_i$, are the mixed strategy row vectors available to player i, where n is the index of possible mixed strategy vectors available to the i_{th} player. $\Theta_1 \times \Theta_2$ is the set of all possible mixed strategy profiles.

It is convenient to denote -i as the index of "all other players" than player i. For each player i, we define a von Neumann-Morgenstern utility (payoff) function u_i: $S_1 \times S_2 \rightarrow \mathbb{R}$ (a function whose domain is the set of pure strategy profiles and whose range is the set of real numbers) so that for each pure strategy $s_{ik} \in S_i$ that the players could choose, $u_i(s_{ik,}s_{-ik})$ is the player i's payoff in the game . Von Neumann-Morgenstern utility functions are a result of the Von-Neumann-Morgenstern utility theorem stating that because of certain widely accepted axioms of rationality, a decision maker considering random outcomes with a known probability distribution will act to maximize the expected value of a function weighing some measure of the benefits of each outcome by the probability of that outcome.

We extend the definition of a payoff function to mixed strategies by using the concept of *expected value*.

[1] For example, if $S_1\{A, B\}$ and $S_2 = \{X, Y\}$, then $S = S_1 \times S_2 = \{(A, X), (A, Y), (B, X), (B, Y)\}$

doi:10.7290/ijns07vrqk

We define the pure strategy payoff matrix $\boldsymbol{U_i}$ **:**

$$U_i = \begin{bmatrix} u_i(s_{iCo,}s_{-iCo}) & u_i(s_{iCo,}s_{-iCs}) & u_i(s_{iCo,}s_{-iIr}) \\ u_i(s_{iCs,}s_{-iCo}) & u_i(s_{iCs,}s_{-iCs}) & u_i(s_{iCs,}s_{-iIr}) \\ u_i(s_{iIr,}s_{-iCo}) & u_i(s_{iIr,}s_{-iCs}) & u_i(s_{iIr,}s_{-iIr}) \end{bmatrix}$$

When player i selects a mixed strategy vector $\boldsymbol{\rho_{in}}$, her *expected payoff*, $E[u_i]$, is the expectation of u_i with respect to the joint probability distribution resulting from the marginal probabilities in the mixed strategy profile ($\boldsymbol{\rho_{in}, \rho_{-in}}$):

$$E[u_i] = \boldsymbol{\rho_{in}}\, \boldsymbol{U_i}(\boldsymbol{\rho_{-in}})^{\boldsymbol{T}}$$

where T denotes transposition.

B. Assumptions

Assumption 1 (Rationality & Intelligence): Both players in this game are rational and intelligent. Rationality entails a player making all decisions with a view to maximizing their expected utility. Intelligence entails that a player knows the rules of the game and can accurately compute payoffs from all combinations of players' actions that can occur in the game.

Assumption 2 (Common Knowledge & Complete Information): Each player in this game knows their own set of strategies and utility function and the set of strategies and utility function of the other player. It is common knowledge to both players that each player in the game knows the set of strategies and utility function of the other player. It is common knowledge that each player in the game is rational, intelligent, and aware of their own set of strategies and utility function. Common knowledge results in circularity of knowledge that can be stated as, "Player 1 knows that the game is being played, player 2 knows that player 1 knows that the game is being played, player 1 knows that player 2 knows that player 1 knows the game is being played, and so on..."

C. Definitions

Definition 1 (Mixed and Pure Strategies):

A *strategy* is a complete and contingent plan determined by a player in advance of starting the game **[7]**. In the simultaneous one-shot game considered here, a *pure strategy*, $\boldsymbol{s_{ik}} \in S_i$, results in only one of the i_{th} player's possible strategies being played with a probability of 1 and all other possible strategies being played with a probability of zero. Each *mixed* strategy, $\boldsymbol{\rho_{in}}$, is a vector of probabilities $\theta_i(s_{ik})$ of the i_{th} player playing each of their pure strategies, so every pure strategy is represented by a unique $\boldsymbol{\rho_{in}}$ and $S_i \subset \Theta_i$ **[8]**.

Definition 2 (Weak Dominance):

A pure strategy s_{ik} or mixed strategy $\boldsymbol{\rho_{in}}$ is weakly dominated if there exists a strategy (pure or mixed) $s'_{ik} \in S_i$ or $\rho'_{in} \in \Theta_i$ such that

$$u_i(s'_{ik}, s_{-ik}) \geq u_i(s_{ik}, s_{-ik}) \; for\; all\; s_{-ik} \in S_{-i}$$
$$u_i(\rho'_{in}, \rho_{-in}) \geq u_i(\rho_{in}, \rho_{-in}) \; for\; all\; \rho_{-in} \in \Theta_{-i}$$

doi:10.7290/ijns07vrqk

Weak dominance results in a solution by the iterated elimination of dominated strategies wherein dominated strategy profiles are eliminated one at a time until only a single undominated strategy profile remains as the equilibrium solution.

Definition 3 (Pure Strategy Nash Equilibrium):

A pair of pure strategy profiles (s^*_{ik}, s^*_{-ik}), are a pure strategy Nash equilibrium if and only if:

$$u_i(s^*_{ik}, s^*_{-ik}) \geq u_i(s_{ik}, s^*_{-ik}) \; for \; all \; s_{ik} \in S_i and \; s_{-ik} \in S_{-i}$$

A game may have several pure strategy Nash equilibria or none.

Definition 4 (Mixed Strategy Nash Equilibrium):

A pair of mixed strategies $(\rho^*_{in}, \rho^*_{-in})$, are a mixed strategy Nash equilibrium if and only if:

$$u_i(\rho^*_{in}, \rho^*_{-in}) \geq u_i(\rho_{in}, \rho^*_{-in}) for \; all \; \rho_{in} \in \Theta_i and \; \rho_{-in} \in \Theta_{-i}$$

Every finite simultaneous one-shot game has at least one mixed strategy Nash equilibrium.

Definition 5 (Max-min Strategy):

Suppose that player i assumes that player -i will know whatever strategy is chosen by player i and respond by playing the strategy that minimizes the payoff to player i, that is, player -i follows the decision rule $\underbrace{min}_{s-ik} \; u_1(s_{ik}, s_{-ik})$. Then player *i*'s best response is to play the strategy resulting in the strategy profile that maximizes the objective function u_1, given the expected behavior of player -*i*. Thus, player *i*'s max-min strategy, $s"_{ik}$ is chosen by the decision criterion:

$$\underbrace{max}_{s"ik} \; \underbrace{min}_{s-ik} \; u_1(s"_{ik}, s_{-ik})$$

For the non-zero sum RDD game developed in this paper, the definition of max-min strategy is restricted to pure strategy profiles. Every zero-sum game has a Nash equilibrium profile of max-min strategies for both players (possibly including mixed strategies), but this result is not obtained for non-zero-sum games. Following Wald **[*10*]**, decision theory literature has presented the max-min criterion as appropriate for decisions under uncertainty.

IV. Game Characteristics and Mapping of Two Approaches

The assumptions and definitions developed in the previous sections apply to this RDD game. The PFRI methodology, applied to a hypothetical facility derived in Rane & Harris **[*3*]**, provides the parameter values for the game theoretical model. Each player is permitted to use pure or mixed strategies. In general, the defender can only afford to harden (or upgrade) defenses of only one of the three high risk radionuclides present at the healthcare facility: cobalt (^{60}Co), cesium (^{137}Cs), or iridium (^{192}Ir). The attacker can attack only one of the three given radionuclides. It is assumed that prior to the start of the game, the baseline defenses required as per 10 CFR Part 37 **[*11*]** are implemented by the hypothetical facility; computation of the success probability of theft (P_s) for the remaining two radionuclides reflects the existing defenses. The source which is in the hardened state is invulnerable to attack.

doi:10.7290/ijns07vrqk

The extended form of RDD game, shown in Figure 2, displays the decision nodes and payoffs for each player in the form of a game tree diagram. The branches of the diagram represent a possible strategy that could be chosen at the corresponding node, and branches terminating on an oval shape are unknown to the other player. This game assumes complete information, which is distinct from perfect information **[*8*]**. Perfect information entails that any player can always observe the actions of the other throughout the game, meaning that in a simultaneous game of perfect information, the players would select their strategies simultaneously and with instantaneous knowledge of the decision made by the other player. The RDD game is simultaneous but has imperfect information, meaning that players select their strategies simultaneously but without being instantaneously informed of the outcome of the other player's decision.

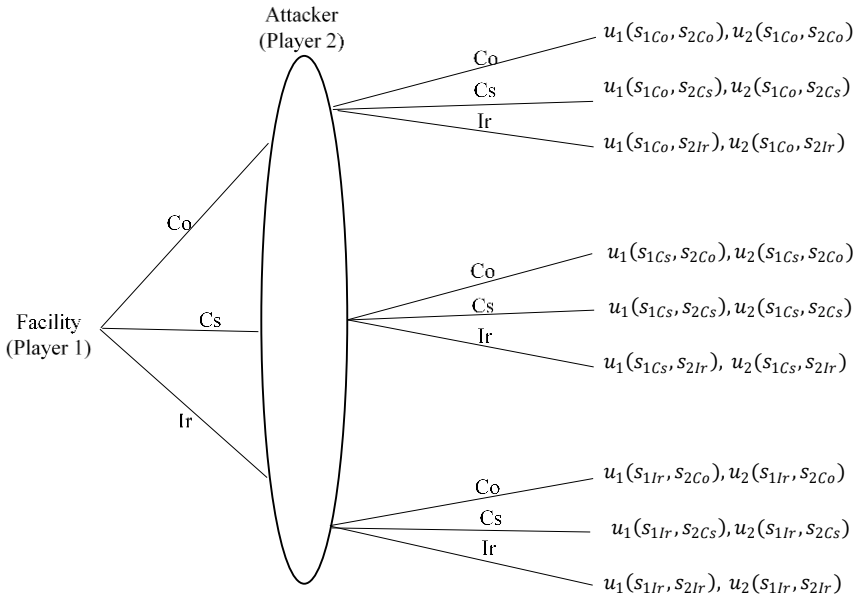

Figure 2. The RDD game tree with decision nodes and payoffs

The pair of utility functions behind each branch indicate the gains and losses of both the defender and the attacker. The assets *Co*, *Cs*, and *Ir* indicate the available decision options at each decision node. Both players, who are assumed to be intelligent and rational agents, will act on the decision option that maximizes their individual payoffs.

The utility functions for the defender and the attacker are derived from the quantitative PFRI model summarized in Section II **[*3*]**. The attacker's and defender's expected utilities are functions of the attacker's success probability of theft (P_s). The attacker's success probability of theft is assigned a value of zero for any pure strategy profile $(s_{1k,}s_{2k})$ where $s_{1k} = s_{2k}$. The defender's utility function, u_1, gives the defender's disutility resulting from loss of life and economic loss consequences:

$$u_1(s_{1k,}s_{2k}) = EU[M_k X_2] = P_s(M_k X_2) \times (-C_{k,net}) \qquad (11)$$

where

M_k Attack the k_{th} radioactive material.
X_2 Intent (theft) from player 2 (attacker)
P_s Attacker's success probability of theft

doi:10.7290/ijns07vrqk

The attacker's disutility from a failed attack outcome is assumed to be -0.1 across all radionuclides and attack scenarios for the purpose of the RDD game. We define u_2, the attacker's utility function:

$$u_2(s_{1k,}s_{2k}) = \mathrm{EU}[\mathrm{M_k X_2}] = \mathrm{P_s}(\mathrm{M_k X_2}) \times \mathrm{U_{tot}}(\mathrm{M_k X_2}) - 0.1(1 - \mathrm{P_s}(\mathrm{M_k X_2})) \quad (12)$$

Where,

M_k	attack the k_{th} radioactive material.
X_2	intent (theft) from player 2 (attacker)
P_s	attacker's success probability of theft
U_{tot}	total utility function assessing the attacker's intentions and radioactive material preferences (physical form and attractiveness).

Note that $u_2(s_{1k,}s_{2k})$ = -0.1 if and only if $s_{1k} = s_{2k}$

The normal form of a two-player game presents the payoffs from each strategy profile in the form of a matrix of ordered pairs giving the payoffs to each player from each pure strategy profile. In principle, the payoff numbers entered in the cells of the RDD matrix (U_{RDD}) are (von-Neumann Morgenstern) expected utilities, computed using Eq (11) and Eq (12).

The normal form of the RDD game is the matrix $\boldsymbol{U_{RDD}}$ of ordered pairs of elements from the payoff matrices $\boldsymbol{U_1}$ and $\boldsymbol{U_2}$:

$$\boldsymbol{U_{RDD}} = \begin{bmatrix} u_1(s_{1Co,}s_{2Co}), u_2(s_{1Co,}s_{2Co}) & u_1(s_{1Co,}s_{2Cs}), u_2(s_{1Co,}s_{2Cs}) & u_1(s_{1Co,}s_{2Ir}), u_2(s_{1Co,}s_{2Ir}) \\ u_1(s_{1Cs,}s_{2Co}), u_2(s_{1Cs,}s_{2Co}) & u_1(s_{1Cs,}s_{2Cs}), u_2(s_{1Cs,}s_{2Cs}) & u_1(s_{1Cs,}s_{2Ir}), u_2(s_{1Cs,}s_{2Ir}) \\ u_1(s_{1Ir,}s_{2Co}), u_2(s_{1Ir,}s_{2Co}) & u_1(s_{1Ir,}s_{2Cs}), u_2(s_{1Ir,}s_{2Cs}) & u_1(s_{1Ir,}s_{2Ir}), u_2(s_{1Ir,}s_{2Ir}) \end{bmatrix}$$

The payoffs of the normal form of the RDD game given below in Table 1 resulted from evaluating the utility functions u_1 and u_2, developed for the hypothetical facility using the PFRI methodology.

Table 1. The RDD game with pure strategy defender-attacker payoffs

RDD game – St. Benedict Healthcare				
	Attacker			
		Co	*Cs*	*Ir*
Defender	*Co*	0, -0.1	-0.15, 0.81	-0.084, 0.44
	Cs	-0.36, 0.89	0, -0.1	-0.084, 0.44
	Ir	-0.36, 0.89	-0.15, 0.81	0, -0.1

The "matching pennies" game is a classic example in game theory without any pure strategy Nash equilibria. The "matching pennies" game, as shown in Table 2, is played between two players – Even and Odd. Each player has a penny and must secretly turn the penny to heads or tails. The players then reveal their choices simultaneously. If the pennies match (both heads or both tails), then Even keeps both pennies, so wins one from Odd (+1 for Even, −1 for Odd). If the pennies do not match (one heads and one tails) Odd keeps both pennies, so receives one from Even (−1 for Even, +1 for Odd) **[*8*]**. Like the "matching pennies" game, the RDD game lacks any pure strategy Nash equilibria. The RDD game has no

doi:10.7290/ijns07vrqk

dominated strategies, so there is no dominated strategy solution or solution resulting from the iterated elimination of dominated strategies (IEDS).

Table 2. A simple example game of "Matching Pennies"

Matching Pennies			
Even	Odd		
		Heads	Tails
	Heads	1, -1	-1, 1
	Tails	-1, 1	1, -1

Although there is not an established solution concept providing a pure strategy solution for the RDD game, applying a variation of the max-min solution concept results in a pure strategy solution that could be of interest to the defender. The max-min criterion states that it is rational for a conservative player to choose the strategy that maximizes their minimum possible payoff in the "worst-case" outcome resulting from the possible strategies of their opponent. The literature on max-min strategies describes them as "safety strategies" or "security strategies" because they enable the player to be certain that they have maximized the lower bound of possible outcomes of an otherwise highly uncertain game.

Since it is common for the health physics profession to take a conservative approach to radiation safety, it seems appropriate for the relatively conservative max-min strategy to be adopted by the facility defender rather than any of the more risk-loving strategies that are available. It is not self-evident that the attacker would also use the max-min strategy. The more aggressive max-max strategy, in which the strategy allowing the maximum possible payoff is chosen, could be a better fit to the attacker psychology. If the defender commits to the max-min strategy, choosing to prevent a worst possible payoff of -0.36 by playing s_{1Co}, the attacker's use of the max-max strategy resulting in the play of s_{2Co} would benefit the defender, giving the defender their best-case payoff of 0.

In the RDD game, the attacker is indifferent among their available pure strategies on the max-min criterion because their worst-case payoff is -0.1 for each pure strategy. Under the complete information assumption, the attacker would know that the defender is conservative. Thus, it would be rational for the attacker to infer that a conservative defender would play s_{1Co} to satisfy the max-min criterion if the game is limited to pure strategies. If the attacker infers that the defender would play a pure strategy of s_{1Co}, the attacker's best response would be to play s_{2Cs}, resulting in a pure strategy equilibrium solution of (s_{1Co}, s_{2Cs}) under a variation of the max-min equilibrium solution concept. Any unilateral deviation by the attacker from (s_{1Co}, s_{2Cs}) would result in a worse payoff for the attacker and a better payoff for the defender.

According to Nash **[*12*]**, every simultaneous one-shot game has at least one mixed strategy Nash equilibrium solution. For any strategy profile that is a Nash equilibrium, neither player could obtain a greater payoff by unilaterally deviating from the strategy profile. Hence player *i* would be indifferent between playing any of their pure strategies against the Nash equilibrium mixed strategy of their opponent, $\boldsymbol{\rho^*_{-in}}$. It follows that for the RDD game there exists a Nash equilibrium mixed strategy profile ($\boldsymbol{\rho^*_{1n}}, \boldsymbol{\rho^*_{2n}}$) that can be obtained from the system of equations:

$$\boldsymbol{\rho^*_{1n}}(\boldsymbol{U_2})^{\boldsymbol{T}}(\hat{\boldsymbol{\imath}})^{\boldsymbol{T}} = \boldsymbol{\rho^*_{1n}}(\boldsymbol{U_2})^{\boldsymbol{T}}(\hat{\boldsymbol{\jmath}})^{\boldsymbol{T}} = \boldsymbol{\rho^*_{1n}}(\boldsymbol{U_2})^{\boldsymbol{T}}\left(\hat{\boldsymbol{k}}\right)^{\boldsymbol{T}}$$

doi:10.7290/ijns07vrqk

$$\hat{\imath}\boldsymbol{U_1}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}} = \hat{\boldsymbol{\jmath}}\boldsymbol{U_1}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}} = \hat{\boldsymbol{k}}\boldsymbol{U_1}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}}$$

where $\hat{\imath}, \hat{\jmath}, \hat{k}$ are unit row vectors. The following system of equations is solved to determine the mixed strategy probabilities that are the components of the vectors $\boldsymbol{\rho}^*_{\boldsymbol{1n}}$ and $\boldsymbol{\rho}^*_{\boldsymbol{2n}}$:

$$\begin{aligned}
&\theta_1(s_{1Co})u_2(s_{1Co},s_{2Co})+\theta_1(s_{1Cs})u_2(s_{1Cs},s_{2Co})+ (1-\theta_1(s_{1Co})-\theta_1(s_{1Cs}))u_2(s_{1Ir},s_{2Co})\\
&= \theta_1(s_{1Co})u_2(s_{1Co},s_{2Cs})+\theta_1(s_{1Cs})u_2(s_{1Cs},s_{2Cs})+ (1-\theta_1(s_{1Co})-\theta_1(s_{1Cs}))u_2(s_{1Ir},s_{2Cs})\\
&= \theta_1(s_{1Co})u_2(s_{1Co},s_{2Ir})+\theta_1(s_{1Cs})u_2(s_{1Cs},s_{2Ir})+ (1-\theta_1(s_{1Co})-\theta_1(s_{1Cs}))u_2(s_{1Ir},s_{2Ir})\\
&= \theta_2(s_{2Co})u_1(s_{1Co},s_{2Co})+\theta_2(s_{2Cs})u_1(s_{1Co},s_{2Cs})+(1-\theta_2(s_{2Co})-\theta_2(s_{2Cs}))u_1(s_{1Co},s_{2Ir})\\
&= \theta_2(s_{2Co})u_1(s_{1Cs},s_{2Co})+\theta_2(s_{2Cs})u_1(s_{1Cs},s_{2Cs})+ (1-\theta_2(s_{2Co})-\theta_2(s_{2Cs}))u_1(s_{1Cs},s_{2Ir})\\
&= \theta_2(s_{2Co})u_1(s_{1Ir},s_{2Co})+\theta_2(s_{2Cs})u_1(s_{1Ir},s_{2Cs})+ (1-\theta_2(s_{2Co})-\theta_2(s_{2Cs}))u_1(s_{1Ir},s_{2Ir})
\end{aligned}$$

After obtaining the mixed strategy probabilities for a Nash equilibrium, the mixed strategy payoffs are computed as follows:

$$E[u_1] = \boldsymbol{\rho}^*{}_{\boldsymbol{1n}}\boldsymbol{U_1}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}}$$
$$E[u_2] = \boldsymbol{\rho}^*{}_{\boldsymbol{1n}}\boldsymbol{U_2}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}}$$

The results of the mixed Nash equilibrium solution are shown in Table 3.

Table 3. The RDD game mixed strategy Nash equilibrium solution

RDD game mixed strategy Nash equilibrium solution			
	mixed strategy probabilities		mixed strategy payoffs
Defender	$\theta_1(s_{1Co})$	0.49	-0.09
	$\theta_1(s_{1Cs})$	0.45	
	$\theta_1(s_{1Ir})$	0.06	
Attacker	$\theta_2(s_{2Co})$	0.13	0.40
	$\theta_2(s_{2Cs})$	0.31	
	$\theta_2(s_{2Ir})$	0.56	

Table.3 shows that the attacker maximizes the expected damage to the defender by attacking *Ir* with probability 0.56. The defender minimizes its expected loss by defending *Co* with probability 0.49. For these choices, the expected return for defending *Co* is -0.09 and the expected return for attacking *Ir* is 0.40. The results of the mixed strategy Nash equilibrium show that if either player deviates from its strategy, then the terrorist adversary can do no better, and his or her opponent (the healthcare facility) can do no worse, than the equilibrium-strategy payoffs.

V. Discussion and Conclusion

The RDD game uses recursive functions to model the adaptive response of terrorist adversary to the defensive countermeasures of healthcare facilities. It's assumptions of rationality, common knowledge, and the availability of mixed strategies may, however, not be realistic in RDD scenarios **[*13*]**. The mixed strategy Nash equilibrium solution of the RDD game has the payoff $u_1(\rho^*_{1n}, \rho^*_{2n}) = -0.09$, whereas the pure strategy solution under a variation of von Neumann's max-min solution concept has the payoff $u_1(s_{1Co}, s_{2Cs}) = -0.15$. The mixed Nash solution is preferable to the pure von Neumann max-min solution if two necessary conditions for its existence obtain: (1) mixed strategies are feasible for both

doi:10.7290/ijns07vrqk

players; and (2) both players correctly believe that their opponent is committed to the mixed strategy Nash equilibrium profile. Conditions (2) is not provided by the definition of common knowledge.

Condition (1) is unlikely to be satisfied for the terrorist attacker or the healthcare defender. There is some evidence that terrorists randomize their strategies, e.g., Timothy McVey claimed that he randomly turned to a phone book page to target the Alfred P. Murrah building in Oklahoma City **[*14*]**. However, it is unlikely that many terrorist adversaries would be sufficiently familiar with game theory to compute Nash equilibrium mixed strategies **[*15*]**. Condition (1) appears unlikely for a real healthcare facility to satisfy due to the difficulty of randomizing defenses, which are typically static and continuously operating at full capacity. Mixed strategies have been implemented for the Department of Homeland Security to randomize patrols or surveillance of vital large-scale infrastructure, e.g., the assistant for randomizing monitoring over routes (ARMOR) deployed at the Los Angeles International Airport **[*16*]**. Although the deployment at healthcare facilities of automated surveillance systems or enhanced security patrols could be randomized, it would be difficult to persuade decision makers to invest in these costly security upgrades only for the purpose of deploying them randomly in support of a mixed strategy.

We have shown that condition (1) is unlikely to be satisfied in a realistic RDD game. If condition (1) is not satisfied, condition (2) cannot be satisfied because both players need to correctly believe that their opponent is committed to a mixed strategy, and such a belief cannot be correct if mixed strategies are infeasible. If the necessary conditions for a Nash equilibrium are unlikely to exist in a real instance of the RDD game, the Nash equilibrium solution is not robust for determining the optimal defense policy of the healthcare facility.

The max-min solution concept is highly robust under conditions of severe uncertainty because it gives the certain result that the lower bound on the uncertain payoffs is maximized. The necessary assumptions for the max-min equilibrium solution to exist in a real RDD game are rationality and common knowledge. Real world players do not possess the perfect rationality and common knowledge of an idealized game-theoretic model, but human behavior in real conflicts between terrorists and security forces is a reasonable approximation of these assumptions **[*17*]**. Thus, we find that the von Neumann max-min solution of (s_{1Co}, s_{2Cs}) is the most prescriptive result of the RDD game from the standpoint of healthcare sector security policy.

If the max-min based prediction about attacker's behavior is wrong, then the defender can only do better ($u_1(s_{1Co}, s_{2Co}) = 0$ *or* $u_1(s_{1Co}, s_{2Ir}) = -0.084$), but not worse, than if the prediction is right. Thus, based on the max-min equilibrium solution of the RDD game, the healthcare facility could either direct its scarce resources towards defending *Co* and accepting the payoff of -0.15 or it could replace cesium blood irradiators by alternative technologies, resulting in a payoff of -0.084.

Consideration of technological alternatives to radionuclide radiation sources has been recommended by national and international organizations like the IAEA, the Nuclear Regulatory Commission (NRC), the National Nuclear Security Administration (NNSA), the Health Physics Society (HPS), and others **[*15*]**. Implementing a policy of replacing the cesium source with an X-ray technology in the hypothetical healthcare facility scenario would both support a more effective outcome of the game and provide an additional incentive to the current cooperative risk mitigation efforts.

As shown in Table. 4, the max-min solution to the updated RDD game after the replacement of cesium blood irradiator with X-ray technology gives a strategy profile $(s_{1Co,}s_{2Ir})$ with the payoffs $u_1(s_{1Co,}s_{2Ir}) = -0.084$ and $u_2(s_{1Co,}s_{2Ir}) = 0.44$. This solution is favorable to the defender because the defender's payoff is the second best possible (their best outcome would be u_1=0) and the attacker's payoff is the second worst possible (their worst outcome would be u_2 = -0.1). The defender's strategy has

doi:10.7290/ijns07vrqk

influenced the attacker to target iridium, which has significantly lower consequences for society than an RDD attack targeting cobalt or cesium.

Table 4. The RDD game reduced matrix upon source (CsCl) replacement

RDD game – reduced matrix upon source replacement			
Defender	Attacker		
		Co	*Ir*
	Co	0, -0.1	-0.084, 0.44
	Ir	-0.36, 0.89	0, -0.1

The RDD game results shows that game-theoretic reasoning can augment risk indexes such as the PFRI by providing decision makers with the capability to optimize their defenses against the predicted behavior of terrorist adversaries. The RDD game gives the defender strategic options that can be interpreted as possible allocations of a defense upgrade available for only one of the three sources at a time. This simplified idealization captures the trade-offs inherent in budgeting scarce security resources. A realistic policy prescription following from the RDD game would be to replace the cesium source with an alternate technology and divide the available security resources equitably between the two remaining sources, cobalt and iridium.

Risk metrics developed from probabilistic risk analysis, such as the PFRI, do not capture the strategic interaction between adversaries that is shown in game theoretical models. However, probabilistic risk analysis provides content for a game theoretic matrix that cannot be provided by game theory alone. The RDD game presented in this paper fills its payoff matrix with the success probability of theft, Ps, and utility functions developed in the prior publication about the PFRI. The, P_s, and utility functions used to compute payoffs for the RDD game are adopted from functions given for the hypothetical medical facility analyzed in the prior publication **[*3*]**, and additional success probabilities of theft for Cs and Ir obtained using the PFRI methodology are presented in this paper. Although great care must be taken to gather reliable information for PFRI studies of particular healthcare facilities, the core idea of mapping the PFRI methodology to a game theoretical model produces sensible insights for allocating defensive resources **[*18*]**. As future work, a risk informed cost-benefit analysis drawing on input from the PFRI and the RDD game can ensure that each healthcare facility uses its security budget optimally to reduce the RDD threat.

VI. Works Cited

1. L. Rajbhandari, E. A. Snekkenes, in *Communications and Multimedia Security*, B. De Decker, J. Lapon, V. Naessens, A. Uhl, Eds. (Springer, Berlin, Heidelberg, 2011), *Lecture Notes in Computer Science*, pp. 147–154, doi:10.1007/978-3-642-24712-5_12

2. L. A. Cox, *Improving Risk Analysis* (Springer New York, New York, NY, 2013; http://link.springer.com/10.1007/978-1-4614-6058-9), vol. 185 of *International Series in Operations Research & Management Science*, doi:10.1007/978-1-4614-6058-9

3. S. Rane, J. Harris, Development of a Potential Facility Risk Index for Radiological Security. *Risk Anal. Off. Publ. Soc. Risk Anal.* **41**, 1257–1273 (2021), doi:10.1111/risa.13625

doi:10.7290/ijns07vrqk

4. *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control: Implementing Guide* (International Atomic Energy Agency, 2015; https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4853274), vol. No. 24-G of *IAEA Nuclear Security Series*.

5. R. L. Keeney, D. von Winterfeldt, A Value Model for Evaluating Homeland Security Decisions. *Risk Anal.* **31**, 1470–1487 (2011), doi:10.1111/j.1539-6924.2011.01597.x

6. M. L. Garcia, *Design and Evaluation of Physical Protection Systems* (Butterworth-Heinemann, ed. 2, 2007; https://www.elsevier.com/books/design-and-evaluation-of-physical-protection-systems/garcia/978-0-08-055428-0), doi:10.1016/c2009-0-25612-1

7. J. Watson, *Strategy: an introduction to game theory* (W. W. Norton & Company, New York, Third Edition., 2013).

8. D. Fudenberg, J. Tirole, *Game Theory* (MIT Press, Cambridge, MA, USA, 1991).

9. J. von Neumann, O. Morgenstern, Theory of Games and Economic Behavior. *J. Philos.* **42**, 550 (1945).

10. A. Wald, Statistical Decision Functions. *Ann. Math. Stat.* **20**, 165–205 (1949).

11. NRC CFR 10 PART 37—PHYSICAL PROTECTION OF CATEGORY 1 AND CATEGORY 2 QUANTITIES OF RADIOACTIVE MATERIAL. *US Nucl. Regul. Comm.* (2021), (available at https://www.nrc.gov/reading-rm/doc-collections/cfr/part037/index.html).

12. J. Nash, Non-Cooperative Games. *Ann. Math.* **54**, 286 (1951), doi:10.2307/1969529

13. V. M. Bier, M. N. Azaiez, Eds., *Game theoretic risk analysis of security threats* (Springer Science+Business, New York, 2009; https://stanford.idm.oclc.org/login?url=http://dx.doi.org/10.1007/978-0-387-87767-9), *International series in operations research & management science*.

14. J. Wasson, C. Bluesteen, Cognitive Defense: Influencing the Target Choices of Less Sophisticated Threat Actors. *Homel. Secur. Aff.* (2017), (available at https://www.hsaj.org/articles/13770).

15. M. Pomper, E. Murauskaite, T. Coppen, *Promoting Alternatives to High-Risk Radiological Sources: The Case of Cesium Chloride in Blood Irradiation* (James Martin Center for Nonproliferation Studies, Washington, D.C., 2014; https://www.nonproliferation.org/wp-content/uploads/2014/03/140312_alternative_high_risk_radiological_sources_cesium_chloride_blood.pdf).

16. J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, S. Kraus, Using Game Theory for Los Angeles Airport Security. *AI Mag.* **30**, 43–57 (2009), doi:10.1609/aimag.v30i1.2173

17. S. D. Guikema, in *Game Theoretic Risk Analysis of Security Threats*, V. M. M. Bier, M. N. Azaiez, Eds. (Springer US, Boston, MA, 2009; https://doi.org/10.1007/978-0-387-87767-9_2), *International Series in Operations Research & Management Science*, pp. 13–31, doi:10.1007/978-0-387-87767-9_2

doi:10.7290/ijns07vrqk

18. S. Meng, M. Wiens, F. Schultmann, (New Forerst, UK, 2014; http://library.witpress.com/viewpaper.asp?pcode=RISK14-013-1), pp. 141–152, doi:10.2495/RISK140131

VII. Authors' Bios and Contact Information

Shraddha Rane
Dr. Shraddha Rane is a Postdoctoral Researcher in the School of Health Sciences at Purdue University. She recently graduated with her doctoral degree in Health Physics with an emphasis in Nuclear Security from Purdue University. Her research interests include risk assessment, accelerator physics, environmental radiological science, and radioactive waste disposal. She received her Bachelor's in Physics from Montana State University, Bozeman and her Master's in Health Physics from Idaho State University, Pocatello. She has worked as a Health Physicist at Waste Control Specialist, Texas and the Washington State Department of Health, Olympia. She has served as a Chapter President for various health physics student chapters. She also served as a Secretary Treasurer for the Homeland Security section of the national Health Physics Society (HPS) for the 2017-2019 term. She is a member of Health Physics Society and the Institute for Nuclear Materials Management. Her email address is srane@purdue.edu**.**

Jason Harris
Dr. Jason Harris is an Associate Professor and Director of the Health Physics Program and Center for Radiological and Nuclear Security at Purdue University. His research interests include several areas related to radiation detection and measurement, nonproliferation, and nuclear security. In 2012, he became the Chair of the International Atomic Energy Agency (IAEA) International Nuclear Security Education Network (INSEN). He serves as an expert for the U.S. Department of State Partnership for Nuclear Threat Reduction (PNTR), lecturing at several professional development workshops throughout the world. He also served on the Advisory Board for the European Master's Program in Nuclear Security, sponsored by the IAEA and European Commission. He teaches courses in radiation detection and instrumentation, health physics, radiation physics, laboratory experimentation, nonproliferation, and nuclear security. He is a member of the Health Physics Society, American Nuclear Society, and the Institute for Nuclear Materials Management. Contact: jtharris@purdue.edu

doi:10.7290/ijns07vrqk