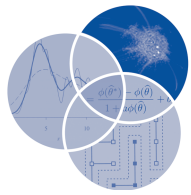
Advanced Review



Game-theoretic computing in risk analysis

Mehmet Sahinoglu,[1]* Luis Cueva-Parra[2] and David Ang[3]

Risk analysis, comprising risk assessment and risk management stages, is one of the most popular and challenging topics of our times because security and privacy, and availability and usability culminating at the trustworthiness of cybersystems and cyber information is at stake. The precautionary need derives from the existence of defenders versus adversaries, in an everlasting Darwinian scenario dating back to early human history of warriors fighting for their sustenance to survive. Fast forwarding to today's information warfare, whether in networks or healthcare or national security, the currently dire situation necessitates more than a hand calculator to optimize (maximize gains or minimize losses) risk due to prevailing scarce economic resources. This article reviews the previous works completed on this specialized topic of game-theoretic computing, its methods and applications toward the purpose of quantitative risk assessment and cost-optimal management in many diverse disciplines including entire range of informatics-related topics. Additionally, this review considers certain game-theoretic topics in depth historically, and those computationally resourceful such as Neumann's two-way zero-sum pure equilibrium and optimal mixed strategy solutions versus Nash equilibria with pure and mixed strategies. Computational examples are provided to highlight the significance of game-theoretic solutions used in risk assessment and management, particularly in reference to cybersystems and information security.

How to cite this article:
WIREs Comput Stat 2012. doi: 10.1002/wics.1205

Keywords: risk analysis; Nash equilibrium; game-theoretic; mixed strategy

INTRODUCTION TO GAMING AND HISTORICAL PERSPECTIVE TO GAME THEORY'S ORIGINS

Game playing is an unlimited topic in scope as old as the ancient human history. Although its first seeds were planted in the latter part of the 19th century, the popularity of game theory skyrocketed in the 20th century. This was a period of devastating wars and conflicts that needed urgently smart solutions with the advent of transistor-led electronics, and further, vast computer storage space and unprecedented computational speed. In the 21st century, the cyber wars brought forward a dire necessity to employ gaming solutions to outsmart the hostile hackers and adversaries, in lieu of former invading troops or bombarding warplanes. In retrospect, the first human hunters were involved in game solutions against their enemies, i.e., carnivorous animal world, who played the same game, all to quell hunger. Gaming may mean many things to different people, such as gambling or simulation or politics and warfare. According to Shubik,[1] the disciplines most heavily involved in the utilization of games have been management science and operations research, psychology, education, political science, sociology, engineering, computer and military science, and economics. The major expenditures, in terms of

*Correspondence to: msahinog@aum.edu

[1]Informatics Institute, 'Cybersystems and Information Security' graduate program, Auburn University at Montgomery, Montgomery, AL, USA

[2]Mathematics Department–CS Option, School of Sciences, Auburn University at Montgomery, Montgomery, AL, USA

[3]Information Systems and Decision Science, School of Business, Auburn University at Montgomery, Montgomery, AL, USA

both time and other resources have been made through military or business or education support.

There is no mystery about the origins of game theory, which is the mathematical study of conflict situations as a *science of rational conflict*.[2] It was, to all intents and purposes, reborn in 1944 as an established field with the publication of a single tough-to-read pioneering book, *Theory of Games and Economic Behavior* by John von Neumann and O. Morgenstern which proposed that most economic questions could be analyzed as games, and first laid out the finite two-person zero-sum game.[3] The 1944 book arrived just about or even a few years before Linear Programming methods came upon the scene in 1947 by George Dantzig who worked in close connection with Theory of Games. This theory was originally proposed by the French mathematician Emile Borel about 1921 as noted in Ref 4. Borel's theory was successfully analyzed by J. von Neumann who proved its key result, the Minimax theorem in 1928. Neumann and Morgenstern in 1944 defined the minimax solution and showed that this solution exists in all two-player zero-sum games in which the interests of players are diametrically opposed with no common interest. Thereupon, Dantzig's simplex method became an important tool both in the practical and theoretical investigations in the theory of matrix games (so-called zero-sum, two-person games) in game theory. Six years after, Nash in 1950 proposed what became known as *Nash equilibrium* as a way of extending game-theoretic analyses known as no-zero-sum games by determining a steady-state solution that no other player can outsmart.[5] Even before 1944, the first studies of games in economics literature were the papers by Cournot in 1838,[6] Bertrand in 1883,[7] and Edgeworth in 1897[8,9] on the pricing and production of an oligopoly, which is a market or industry dominated by a small number of sellers.

In the 19th century models of Cournot and Bertrand, the strategies of the players were simply their choices of outputs and prices. One of the insights of von Neumann and Morgenstern in the middle of a new 20th century was that the strategies of a game could also be more complex plans for contingent reconciliatory actions; for example, *I'll cut my price tomorrow, if you cut yours today*. Selten, an Esperantist (foremost proponent of Esperanto language) and the 1994 Nobel laureate awarded for equilibrium notions in dynamic games in 1965[10,11] as well as Harsanyi in 1967, introduced concepts widely used in recent years.[12] Harsanyi proposed a way in which all players know the payoff functions of the other players, to model situations of incomplete information where the players are unsure of one another's payoffs. Harsanyi's Bayesian Nash equilibrium is precisely the Nash equilibrium of the imperfect-information representation of the game, and is the cornerstone of game-theoretic analyses as noted in Ref 13, p. 210. Nash, Harsanyi, and Selten shared the Nobel Prize in economic sciences in 1994.[14] According to Osborne and Rubinstein,[15] game theory is a bag of analytical tools to help understand the phenomena that we observe when decision makers interact, whereby the models of game theory are highly abstract representations of classes of real-life situations. This means game theory uses mathematics to express its ideas formally but mathematical results are interesting only if they are confirmed by human intuition. In short, game theory deals with decisions in conflict situations. Interest in game theory as a *science of rational conflict* is extremely widespread in our age of competition, strategy, and gamesmanship.[12] "*Does Game Theory Work?*" asks Binmore and responds that Game Theory does not work in the laboratory.[16] People do not play Nash equilibrium and they do not use their *maximin* or *minimax* strategies in two-person zero-sum games. But who can claim and guarantee that any theory can work in all environments, just as Newton's laws of motion do not predict well at the bottom of the sea, and also were modified by Einstein's relativity theory in 20th century? Therefore, game theory cannot be reasonably expected to work in unfavorable environments in which its tacit assumptions have whatsoever no chance of being true. To the eye of the game theorist, there exist four essential elements for instance in the chess or poker game: (1) two players, (2) opposite interests, (3) finite game, and (4) no surprises.[17,18] However, modern game theory has stretched its limits to new concepts by Aumann (rational expectations)[19] and Kadane (subjective probability)[20] and more. Aumann writes: (1) If the game is not two-person zero-sum, even if there is just one Nash equilibrium, it is not clear what players should expect as payoff in an *n*-person game. (2) Nash equilibrium is a solution for strategic games but rational expectations are more fundamental for the one-shot game if not repeated.

History of Applications of Game Theory in Cyber-Security Risk Analysis

Cybersystems security which did not exist when game theory debuted has recently evolved into a complex and challenging problem. The area of cyber-network defense mechanism design has been receiving immense attention from the research community for more than two decades ever since the first Internet message was delivered thanks to DARPA research (Defense Advanced Research Projects Agency) www.**darpa**.mil. However, the cyber-security problem is far from completely solved. Scientists are exploring the applicability

of game-theoretic approaches to address the security issues and some of these approaches look promising. The goal of the ongoing research is to manage the cybersystems against malicious cyberattacks by using game theory and computationally intensive algorithms. The initial papers, among many others specifically on game-theoretic risk analysis, started appearing a decade ago not long after the tragic events of 9/11 in 2001 as in a literature survey.[21] This trend continued in 2002 as applied to information warfare by Hamilton, Saydjari et al.[22,23] Concurrently, the role of trust and game strategies as implemented to network security by Lye and Wing[24,25] appeared. Following, Cavusoglu et al.[26] and Patcha and Park in 2004 wrote on IT security and mobile networks respectively.[27] In 2005, Jormakka and Mölsä published their pioneering paper titled *Modeling Information Warfare as a Game* where they treated *Terrorist Game: Bold Strategy* concept with Nash equilibrium.[28] Sahinoglu also in 2005 pioneered with his quantitative and hybrid Security Meter computational model[29] at the risk assessment stage to be followed up by another at the risk management stage.[30] His findings were followed by other pertinent game-theoretic risk applications.[31–36] After 2004, research on *Adversarial Risk Analysis* followed until the present time due to a growing interest owing to a multiplicity of terror activities on the rise.[37–39] Massive Stackelberg security games,[40,41] decision-theoretic rough sets[42] and attack-defense models, which were oriented to network security risk assessment were a few of the examples in search of a working algorithm to quantify and manage risk.[43,44] Later in 2009 to 2011 multiple papers followed by a group of game-theoretic researchers on defense-related game theory.[45–52] Luo et al. in 2010 published a non-cooperative non-dynamic game with incomplete information.[53] Recently, problems in counterterrorism and corporate competition have prompted research that attempts to combine math-statistical risk analysis with game theory in ways that support practical decision making. Wang and Bank's latest article applies these methods of adversarial risk analysis to the problem of selecting a route through a network, in which an opponent chooses certain vertices for ambush.[54] However, recently well-proposed methods are missing the link from theory to framing and transforming theorems into *working expert systems* or *software programs* to generate solid results that are commercially usable and cost efficient. Game theory, therefore, is a branch of applied mathematics that attempts to analytically model the rational behavior of intelligent agents in strategic situations, in which an individual's success depends on the decisions of others. While initially developed to analyze competitions in which one individual does better at another's expense, it recently evolved into techniques for modeling a wide class of interactions, characterized by multiple criteria.[14,15]

INTUITIVE BACKGROUND—CONCEPTS, DEFINITIONS, AND NOMENCLATURE OF GAME THEORY

Game Theory Definitions

A branch of mathematics, devoted to the logic of decision making in social or political interactions, concerns the behavior of decision makers whose decisions affect each other. Note that each decision maker has only partial control over the outcome. Game theory is a generalization of decision theory where two or more decision makers compete by selecting each of the several strategies. Decision theory whereas is essentially one-person game theory. In general, any game involves the following. *Players*: An individual or a group of individuals can be considered a player such as individuals or teams, companies, political candidates, and contract bidders. *Actions (strategies)*: The set of moves available to choose from for each player. *Outcomes*: An outcome in a game is the act of each player choosing a move from its action set so that numerical payoffs reflecting these preferences can be assigned to all players for all outcomes. *Preferences*: Each player prefers some outcome to others based on payoffs or utilities associated with these outcomes. In spite of its name, game theory is not specifically concerned with recreation and pastimes (like children's games) and a less misleading name would have been the *theory of interdependent decision making*, but it is too late to rename game theory without risking even worse confusion.[53] A simple example will help to provide an intuitive understanding of the kinds of social interactions involving interdependent decision making, which falls within the purview of game theory. We will start with the most popular two-player zero-sum games. Zero-sum means that the gain (or loss) for one player is equal to the loss (or gain) for the other player with diametrically opposite interests. In other words, what one player wins becomes what the other player loses.

A Price War Example

Two retail companies are each trying to carve out a larger slice of a market for which they compete. Each has to decide on a strategy in ignorance of the other's decisions whether or not to: (1) increase advertising its product, (2) provide quantity discounts, or (3) extend warranty terms. We demonstrate a two-player, zero-sum game and its solution of the two companies

TABLE 1 | Modified Payoff Table Showing the % Gain (loss) in Market Share for Firm A (B)

A / B	% Increase Advertising: b_1	% Quantity Discounts: b_2	% Extended Warranty : b_3	ROW MINIMUM
% Increase Advertising a_1	4	3	2	**2 = Maximin**
%Quantity Discounts a_2	–1	4	1	–1
Extended Warranty a_3	5	–2	5 **(0)**	–2
COLUMN MAXIMUM	5	**4 = Minimax**	5 **(2 = Minimax)**	*Result:* **The solution to the game is for Firm A to raise advertising (a_1) and for Firm B to extend warranty (b_3) by 2%**

Firm A's market share will increase by 2%. Firm B's shall decrease by 2%. 2–4%, a pure strategy does not exist initially. It is not optimal for each firm to predict and select a pure strategy regardless of what the other does. By trial and error, optimal solution is a balanced strategy (Maximin = Minimax = 2).

competing for market share. A payoff table showing the percentage gain in the market share for Company A for each combination of strategies is shown in Table 1. Any gain in market share for Company A is a loss in market share for Company B because it is a zero-sum game.[55,56]

Minimax strategy exists if Maximum (row minimums) = Minimum (column maximums). The game is said to have a saddle or an equilibrium point. A game has a *pure strategy solution* when the players cannot improve their payoff by changing to a different strategy. What to do when pure strategy does not exist?

Identifying an Optimal Mixed Strategy Solution

With a mixed strategy, each player selects its strategy according to a probability distribution. In the market share example in Table 1, each company will first determine an optimal probability distribution for selecting whether to increase advertising, provide quantity discounts or extend warranty. Then, when the game is played each company will use its probability distribution to randomly select one of its three strategies. Now consider the game from the point of view of Company B to select one of its strategies based on the following probabilities: PB_1 (to select strategy b_1), PB_2 (to select strategy b_2), PB_3 (to select strategy b_3). Since the objective of Company B is to minimize its expected loss, *LOSSB*, we have the following linear programming (*LP*) model. Note, one can guess that the value of the game will be between 2% (Maximin) and 4% (Minimax) in Table 1 before solving the mixed strategy problem by the set of linear equations:

$$PB_1, PB_2, PB_3, LOSSB \geq 0,$$

$$\text{where } Min\ LOSSB, \text{ s.t. (subject to) :}$$

$$4PB_1 + 3PB_2 + 2PB_3 - LOSSB <= 0 \text{ (Strategy } a_1)$$

$$-1PB_1 + 4PB_2 + 1PB_3 - LOSSB <= 0 \text{ (Strategy } a_2)$$

$$5PB_1 - 2PB_2 + 5PB_3 - LOSSB <= 0 \text{ (Strategy } a_3)$$

$$PB_1 + PB_2 + PB_3 = 1;$$

Solved *linear programming* results using the CD-ROM Management Scientist in Ref 55

$$PB_1 = 0, PB_2 = 0.375, PB_3 = 0.625,$$

$$LOSSB = 2.375 \text{ (objective function value).}$$

Results of the Two-Player Mixed Strategy Game

Firm *B*'s optimal mixed strategy is to provide quantity discounts (b_2) with probability 0.375, extend warranty (b_3) with probability 0.625 and should not increase advertising b_1 with probability 0. Expected loss of market share for Firm B of this mixed strategy is 2.375% or a gain of 2.375% for Firm A. This tableau is in equilibrium. Firm B (or A) cannot improve the game by changing the B's (A's) probabilities. The expected B-loss (or A-gain) of this mixed strategy is an in-between value of 2.375%, which is better than

Firm B's best pure strategy (b_2) with minimax: 4% of share in the payoff table or A's maximin: 2%.

Other solutions to games exist besides two-player zero-sum strategy for Maximin = Minimax.[3,55,57]

Backward Induction (Solution Concept for Extensive Form Games)

Steps similar to Bellman's dynamic programming are: (a) determine the optimal choices in the final stage K for each history h^K; (b) go back to stage $K-1$, and determine the optimal action for the player on the move there, given the optimal choice for stage K; (c) *roll back* until the initial stage is reached ([55]Chap. 18; [57]p. 23/43).

Nash Equilibrium: NE (Solution Concept for Normal Form Games)

In summary, the game solution theory we review has two components. First, each player chooses her/his action according to the model of rational choice, given her/his belief about the other player's actions. Second, every player's belief about the other players' actions is correct. These two components are embodied in the following definitions. *Definition* 1 (Ref 15, p. 22): An action profile a^* with the property that no player i can do better by choosing an action different from a_i^* given that every other player j adheres to a_j^*. Nash equilibrium of a strategic game is an action profile in which every player's action is optimal given every other player's action. It is a steady state of an idealized situation. Expressed differently, Nash equilibrium embodies a stable social norm: if everyone else adheres to it, no individual wishes to deviate from it. Using a new notation, we can restate the condition for an action profile a^* to be a Nash equilibrium as follows. *Definition* 2 (Ref 15, p. 23): The action profile a^* in a strategic game with ordinal preferences is a Nash equilibrium if, for every player i and every action a_i of player i, a^* is at least as good as according to player i's preferences as the action profile $(a_i, a^* - 1)$. Player i chooses a_i and every other player j chooses a_j^*.

Equivalently, for every player i, $U_i(a^*) \geq U_i(a_i, a_{-1}^*)$ for every action a_i of player i, where U_i (U for utility) is a payoff function that represents player i's preferences. This definition implies neither that a strategic game necessarily has Nash equilibrium, nor that it has at most one. Examples in this review show that some games have a single Nash equilibrium, some possess none, and others have plenty Nash equilibria. Nash equilibrium as a much broader concept is achieved if an operation point is reached where each player is giving her/his best response facing her/his opponents' strategies. That is, for none of the players there is a unilateral incentive to change her/his strategy, given that the strategy chosen by all opponents are fixed. In other words, each player's strategy i is a best reply to the strategies of the others.[58]

Mixed Strategy of Probabilities in Contrary to Two Player-Zero Sum Solution for Strategic Games

Risk management with a mixed strategy is examined as an alternative to two-player zero-sum if one does not exist. A *pure strategy* provides a complete definition of how a player will play a game as in a two-player zero-sum solution. In particular, it determines the move a player will make for any situation she/he could face. A player's strategy set is the set of pure strategies available to that player. A *mixed strategy* is an assignment of a *probability* to each pure strategy or a probability distribution over the player's actions. This allows for a player to randomly select a pure strategy. Since probabilities are continuous, there are infinitely many mixed strategies available to a player, even if their strategy set is finite. One can regard a pure strategy as a degenerate case of a mixed strategy, in which that particular pure strategy is selected with probability 1 and every other strategy with probability 0. Not all two-player zero-sum games have a saddle point minimax = maximin, as is shown in Table 2 where we observe that minimax

TABLE 2 | Two-Player Mixed Strategy Game Example

Column →	1	2	Row Min
Row ↓	**β=5/8**	**1-β=3/8**	↓
1 **α=3/8**	20	–30	–30
2 **1–α=5/8**	–10	20	–10
Col Max→	20	20	

$\geq$ maximin.[1] Von Neumann extended the concept of both saddle point and strategy by considering probability mixes of strategies called mixed strategies. Von Neumann also argued that the correct play for Person 1 in a game such as shown in Table 2 below would be to use a random device (such as coin or pair of dice) to generate the appropriate odds. In this case select strategy 1 with a probability of 3/8 and strategy 2 with a probability of 5/8. For example, in a 2×2 setting against any strategy of Person 2, this gives Person 1 an expected gain in a scenario where risks are chosen as in Table 2 to assure Nash equilibrium to be proven in Section *Random Probabilistic Selection for Nash Mixed Strategy Equilibria—Various Scenarios*.

$(3/8)(20)+(5/8)(-10) = 5/4$ (against 1 of Person 2),

$(3/8)(-30)+(5/8)(20) = 5/4$ (against 2 of Person 1).

We plan to implement a varying range of mixed strategy solutions, including a Nash equilibrium scenario, as a steady state to see the impact so as to compare with a two-player zero-sum solution. A mixed strategy equilibrium predicts that the outcome of a game is stochastic, so that for a single play its prediction is less precise than that of a pure strategy. How the Nash equlibrium solutions may be derived for several examples as alternatives to the conventional mixed strategy is illustrated in the following text.

RANDOM PROBABILISTIC SELECTION FOR NASH MIXED STRATEGY EQUILIBRIA—VARIOUS SCENARIOS

Defender decides whether to use selection combination or not. Adversary decides whether to game the combination or the single classifier. We use random probabilistic selection based on random primitive as a defense against gaming of the selector. Let us consider a static game in mixed strategies where both players randomize between the two options by solving the game for optimal randomization probability for each player. Game theory is one of the possible ways to study information warfare with mathematical models. Modeling Information Warfare as a Game by Jormakka and Mölsä[28] presents four example games which illustrate the different requirements for an effective playing strategy in information warfare. These games determine how *a bold playing strategy can lead to domination, how a mixed playing strategy can reduce domination*, how it can be useful *to play a dominating strategy only part of the time*, and how *excessive domination can lead to rebels where all playing parties lose*.

Random Probabilistic Selection

The possible Nash equilibria involving mixed strategies can be found by differentiating payoff functions as follows:

α—the probability of adversary gaming the selector

β—the probability of classifier using the selection combination

Expected cost of the payoff matrix:

$$\Pi_C = \alpha\beta c_{11} + (1-\alpha)\beta c_{12} + \alpha(1-\beta)c_{21} + (1-\alpha)(1-\beta)c_{22}$$

The Nash equilibrium (α, β) can be obtained by solving the simultaneous equations $\frac{\partial \Pi_C}{\partial \alpha}$ and $\frac{\partial \Pi_C}{\partial \beta}$ for continuous variables α and β. Application of differential calculus to Table 2 to determine the optimal multipliers for Nash equilibrium:

$$\Pi_C = \alpha\beta(20) + \alpha(1-\beta)(-30) + (1-\alpha)\beta(-10) + (1-\alpha)(1-\beta)20$$

$$\frac{\partial \Pi_C}{\partial \alpha} = \beta(20) + (1-\beta)(-30) + \beta(10) - 20 + \beta(20) = 0 \quad (1)$$

$$\frac{\partial \Pi_C}{\partial \beta} = \alpha(20) + \alpha(30) + (1-\alpha)(-10) - 20 + \alpha(20) = 0 \quad (2)$$

Solution: $\alpha = 3/8$; $\beta = 5/8$, same as the mixed strategy of probabilities selected randomly in Table 2. QED.

Does Nash Equilibrium (NE) Exist for the Company A/B Problem in Table 1?

No, it does not. Following a battery of analyses with Nash differential equations:

$$\Pi_C = \alpha_1\beta_1(4) + \alpha_1\beta_2(3) + 2\alpha_1(1-\beta_1-\beta_2) + \alpha_2\beta_1(-1) + \alpha_2\beta_2(4) + \alpha_2(1-\beta_1-\beta_2) + 5\beta_1(1-\alpha_1-\alpha_2) - 2\beta_2(1-\alpha_1-\alpha_2) + 0$$

$$\frac{\partial \Pi_C}{\partial \alpha_1} = \frac{\partial \Pi_C}{\partial \alpha_2} = \frac{\partial \Pi_C}{\partial \beta_1} = \frac{\partial \Pi_C}{\partial \beta_2} = 0$$

- $+2\beta_1 + \beta_2 = -2$
- $-2\beta_1 + 3\beta_2 = -1$
- $-3\alpha_1 - 7\alpha_2 = -5$
- $3\alpha_1 + 5\alpha_2 = 2$

TABLE 3 | Matching Pennies

Player 1↓/ Player 2→	Head (β)	Tail ($1-\beta$)
Head (α)	1, −1	−1, 1
Tail ($1-\alpha$)	−1, 1	1, −1

$\alpha_1 = \frac{-11}{6}$; $\alpha_2 = \frac{3}{2}$; $\alpha_3 = \frac{4}{3}$ are infeasible; $\beta_2 = \frac{3}{4}$ but one of $\beta_1 = \frac{-11}{8}$ and $\beta_3 = \frac{13}{8}$ is negative with no feasible solution.

Therefore a Nash mixed strategy equilibrium may not always exist. *Not every strategic game has a Nash equilibrium* by Osborne and Rubinstein; A Course in Game Theory as the famous game titled Matching Pennies demonstrates (Ref 15, Chap. 2, p. 19). The conditions under which the set of Nash equilibria of a game are nonempty have been investigated by Kakutanis' fixed point theorem of 1941 (Ref 15, Chap. 2, p. 20).

An Example: Matching Pennies

If two players choose the same face, player 2 pays person 1 a $1. If different faces, player 1 pays player 2 a penalty of $1 as in Table 3.

Note, each person cares about the money he or she receives. Such a game where the players' interests are diametrically opposed is called strictly 'competitive'. The game 'matching pennies' has no Nash equilibrium with none of the cubicles holding equality. That is, Nash equilibrium isolates no steady state as follows.

Since the actions can only be discrete (0 or 1), the payoff function is non-differentiable. The same result of no *Nash equilibrium* is confirmed in words in Ref 15, p. 17. If $\alpha = 1$, $\beta = 1$, $\Pi_1 = 1$ and $\Pi_2 = -1$ as in the payoff matrix for i (first row) $= 1$, j (first column) $= 1$ etc.

Another Game: The Prisoners' Dilemma

The Prisoners' Dilemma[15,59] game has two players (the prisoners): George and Tom. Each of them has two possible strategies: to confess the other or not. Each of them should concurrently decide which one of his strategies to follow (without knowing the choice of the other). Their choices determine their gain: If they both confess, each gets 1 year in prison, but if only one confesses, he will be freed (zero prison time) and used as a witness against each other, who will receive a sentence of 4 years. Finally, if neither confesses, they both get 3 years in prison for a minor offense. See Table 4.

Thus, the action (*Confess*, *Confess*) consists of best response strategies for all players of the game with the least prison time. Whatever one player does, the other prefers *Confess* to the action of *Don't Confess*, so that the game has a unique Nash equilibrium (*Confess, Confess*). This action constitutes a Nash equilibrium of the game. Since all players use a single strategy in this profile, it is called *pure profile or strategy*. That is, if $\alpha = 0$, $\beta = 0$ to represent (Confess, Confess at $i = 2$, $j = 2$); $\Pi_1 = 1$ and $\Pi_2 = 1$ will yield the least penalty of 1 year prison for each. The differentiation to find other solutions is out of question since the two actions (0 or 1) are discrete; therefore, payoff functions are discontinuous and not differentiable.

Finding Nash equilibrium in this game seems to be not a difficult task. But in general, there are more than two players involved with much more complicate payoff functions to lead to difficulties to find Nash equilibrium.

Games with Multiple Nash Equilibria (Terrorist Game: Bold Strategy Can Result in Domination)

The main contribution of this game is to show that a game with more than one conflicting Nash equilibria can only end up in domination. In a symmetric warfare

TABLE 4 | The Prisoner's Dilemma

Player 1↓/ Player 2→	Don't Confess (β)	Confess ($1-\beta$)
Don't Confess (α)	3, 3	0, 4
Confess ($1-\alpha$)	4, 0	1, 1

TABLE 5 | Terrorist Game Example between *T*: Terrorist and *G*: Government

Column (G) →	1	2	Row Min
Row (T) ↓	*action* π_1 with p_G	*action* π_2 with $(1-p_G)$	
1 *action* π_1 with p_T	*(–1, –1)**	*(–5, 0)***	*–5*
2 *action* π_2 with $(1-p_T)$	*(1, –5)****	*(–10, –10)*****	*–10*
Col Max→	*1*	0	

at least one of the players (who are rational) is expected to be in a weaker position then the other players. Terrorist (T) capture hostages and threaten to blow up the hostages if the requirements of the terrorist are not accepted. The government (G) proposes that terrorists should surrender and put to jail. Both players have strategies or actions π_1 and π_2. The strategy π_1 *means accepting what the other player suggests: terrorists surrender or the government accepts the requirements* (e.g., *pays the ransom*). The strategy π_2 means *rejecting what the other player suggests: terrorists kill the hostages or the government rejects to negotiate*. The payoffs are the following by Jormakka and Mölsä[28]:

Note, $^*G$ accepts ransom; T surrenders but goes to jail but gets benefit. Both get -1. $^{**}G$ rejects ransom; T surrenders and goes to jail. T gets -5 and G gets 0. $^{***}G$ accepts the ransom; hostages are free. T gets free. T gets 1 and G gets -5. $^{****}G$ rejects ransom; T kills hostages and themselves. Both get -10. Let us assume T plays mixed strategy $(p_T\pi_1,(1-p_T)\pi_2)$ where $0 \le p_T \le 1$. This signifies that T plays π_1 with the probability of p_T and π_2 with the probability of $(1-p_T)$. G plays the mixed strategy $(p_G\pi_1, (1-p_G)\pi_2)$ where $0 \le p_G \le 1$. The expected payoff v_T for the row bound T is given as follows:

$$\begin{aligned} V_T &= -p_T p_G - 10(1-p_T)(1-p_G) - 5p_T(1-p_G) \\ &\quad + (1-p_T)p_G \\ &= p_T(5-7p_G) - 10 + 11p_G, \end{aligned}$$

And the expected payoff V_G for the columnar G is

$$\begin{aligned} V_G &= -p_T p_G - 10(1-p_T)(1-p_G) - 0p_T(1-p_G) \\ &\quad - 5(1-p_T) \\ p_G &= p_G(5-6p_T) - 10 + 10p_T \end{aligned}$$

The Nash equilibrium points (p_T, p_G) for this game are computed by analyzing the best-response correspondences $p_T{}^*(p_G)$, which is the value of p_T that maximizes $v_T(p_G)$ and also analyzing $p_G{}^*(p_T)$, which is the value of p_G that maximizes $v_G(p_T)$. These correspondences describe how the optimal mixed strategy selection probability depends on the opponents' probability. First we identify the pure strategy Nash equilibria:

$p_T{}^*(0) = 1$ and $p_G{}^*(1) = 0$: Nash equilibrium point is (1, 0)

$p_T{}^*(1) = 0$ and $p_G{}^*(0) = 1$: Nash equilibrium point is (0, 1)

The possible Nash equilibria involving mixed strategies can be found by differentiating the payoff functions for the continuous vector $(p_T,p_G)^T$:

$$\frac{\partial v_T}{\partial p_T} = 5 - 7p_G = 0 \rightarrow p_G = \frac{5}{7}$$

$$\frac{\partial v_G}{\partial p_G} = 5 - 6p_T = 0 \rightarrow p_T = \frac{5}{6}$$

The Nash equilibria are thus the following multiple points (1, 0), (0, 1), $\left(\frac{5}{6}, \frac{5}{7}\right)$. These points reflect the intersection points of the best-response correspondences. The payoffs (v_T, v_G) at the equilibrium points are $(-5, 0)$, $(1, -5)$, $\left(-\frac{15}{7}, -\frac{10}{6}\right)$. The two Nash equilibria points with pure strategies (π_1, π_2) and (π_2, π_1) give the best and highest amidst the available payoffs for v_G and v_T respectively. Thus, the third equilibrium point is not in interest for neither player. As such, however, these results do not yet provide any unique solution to this static game.

A bold strategy can however result in a unique solution in the long term when the static terrorist game is repeated. What is a bold strategy? Let us assume that G is bold and always plays π_2 (rejecting the rival so that it will not negotiate with T). Player T may not believe that G will play boldly, and T may try π_2 for

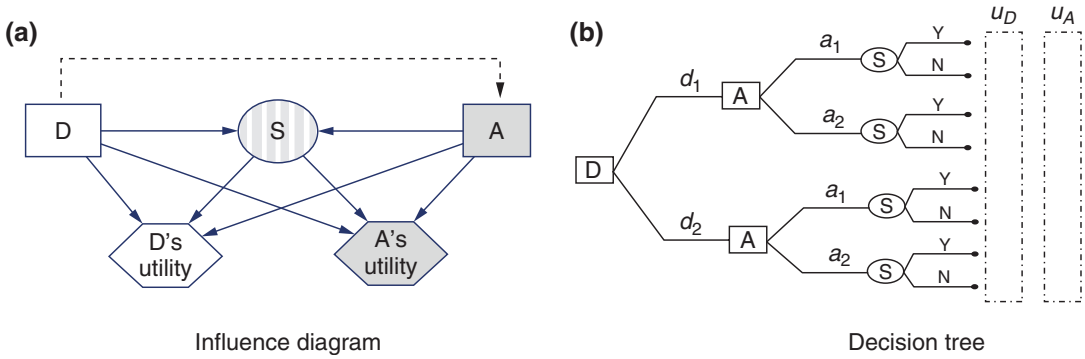


FIGURE 1 | The Defend–Attack sequential decision game by Rios, Rios, and Banks, and influence diagram (a), and decision tree (b) representations.

finitely many times. But if G sticks on to playing π_2, T will eventually finish with a finite negative gain and T will have to start playing π_1 in order to minimize the losses. This familiar real-life game can only end up in domination, where T accepts that G always plays π_2, and will accept losing on this game, or in blowing up hostages and terrorists. Then rational player T must always play π_1. A bold rational player always wins over the less bold rational player in the long term when the terrorist game is repeated. The cause for asymmetric warfare is often the domination in the first place.

There exist three other examples such as: (1) Evildoer Game (*Mixed Defense Strategies Can Reduce Domination*), where there are two players (an attacker and a victim) with two possible choices of each and no pure Nash equilibrium. (2) Vandal Game (*Domination Can Have a Limited Time Span*), where Jormakka and Mölsä[28] do not consider defense strategy but only the fact that the victim will simply not use the system (say, network) and not suffer from the attack.[58] (3) Rebel Game (*Extreme Domination Can Result in Rebellions*), where the dominating solution is expected to cause extremely high costs to the weaker party, who in turn will eventually start to rebel. This may fire back at the dominator!

ADVERSARIAL RISK ANALYSIS (ARA) MODELS

Applications in counterterrorism and corporate competition have led to the development of new methods for the analysis of decisions when there are *intelligent opponents and uncertain outcomes*. This field represents a combination of statistical risk analysis and game theory, and is sometimes called *adversarial risk analysis* (ARA). Prevalent methodologies are based on *game theory, decision analysis, or conventional risk analysis*, emphasizing separate aspects of the analysis. Rios, Rios, Banks[38,39] describe a unified framework for the analysis of decisions under uncertainty *in presence of intelligent adversaries*. The case of a Defend–Attack situation, a sequential decision game is presented in which Daphne (Defender) chooses a defense in $D = \{d1, d2\}$ and then Apollo (Attacker), having observed the defense, chooses an attack in $A = \{a1, a2\}$. The only uncertainty is a binary outcome S representing the success or failure of the Attack. Thus, the consequences for both players depend on the success of his/her attack. Figure 1 shows an influence diagram and a decision tree representing this situation. The arcs into a utility node represent functional dependence.

First, the authors describe how standard game theory solves the Defend–Attack sequential decision game. The game-theoretic approach to ARA requires the probability assessment over S, conditional on (d, a). As Daphne and Apollo may have different assessments for success S, these are $pD(S = 1 \mid d, a)$ and $pA(S = 1 \mid d, a)$, respectively. To compute the Nash equilibrium, one needs the expected utilities of the players at node S of the tree in Figure 1. As a simple, realistic, and specific case of ARA, they consider two applications in auctions. The first is non-adversarial but introduces the basic ideas, and another, the adversarial case. Moreover, it applies the ARA framework to a simultaneous decision-making problem in which the assessment of probabilities on the adversary's actions needs to be more elaborate than in the sequential Defend–Attack decision game.

Suppose now that Daphne and Apollo are bidding against each other. Each knows her/his own valuation of the auctioned object but does not know the valuation of the other. Each submits their bid in a sealed envelope without knowing the other's bid, and the winner is the highest bidder. This simultaneous decision-making situation is shown in the influence diagram in Figure 2 and elaborated in Figure 3.

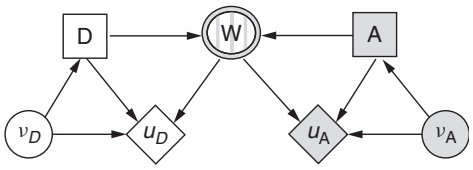


FIGURE 2 | ID of the sealed bid auction problem.

Harsanyi's approach on the other hand leads to the solution concept of Bayes–Nash equilibrium for games with incomplete information, based on the assumption that players share a common prior, which in this case requires those players disclose, inter alia, their true beliefs about the other player's valuation.[12] Thus, Daphne's probabilistic assessment of Apollo's valuation and Apollo's probabilistic assessment of Daphne's valuation would be common knowledge. Only under this assumption it is possible to compute the solution. See also Rothkopf for a related discussion concerning the role of game theory in auctions.[60] The Rios, Rios, and Banks approach[38,39] seems to be more realistic than Harsanyi's. Rios, Rios, and Banks have described a Bayesian approach to adversarial risk analysis problems and modified influence diagrams to represent these situations. They have illustrated it with applications in the context of terrorism, with a sketch of the Defend–Attack model, and bidding in price-sealed auctions. They have focused on two-person games, but the ideas directly extend to harder and more realistic problems as well as to *n*-person games. ARA is a new branch of collaborative statistics. Another paper by Banks and Harris[37] contend that the classical game theory focuses upon a single game, but in many situations such as counterterrorism, it is appropriate to plan for a repeated play as Aumann claims.[19] The game problems are numerous and the applications are important. The authors, Rios, Rios, and Banks believe that the Bayesian perspective has important contributions to make in this arena, and that their formulation is more realistic than the traditional Nash equilibrium analysis in Operations Research or the *ad hoc* decisions that are commonly made in practice by federal agencies and corporate executives.

AN ALTERNATIVE MODEL: SAHINOGLU'S SECURITY METER (RISK-O-METER) FOR GAME-THEORETIC APPLICATIONS TO ASSESS AND MANAGE RISK BY MIXED STRATEGY USING NEUMANN AND NASH EQUILIBRIA

Neumann's Mixed Strategy Solutions to Risk-O-Meter (RoM) Assessment and Management Algorithm

In conventional qualitative risk analyses, assets can be classified on a scale of *crucial-critical* or *very significant*, *significant,* or *not significant*. Vulnerabilities and associated threats can be rated on a scale of *highly likely*, *likely*, *unlikely*, or *highly unlikely*. On the subject of countermeasures and risk mitigation, the qualitative approach is from *strong* (*high*) *to acceptable* (*medium*) *and unacceptable* (*low*). At an Air Force Base gate where to the principal author once commuted, the billboard indicated protection levels: *ALPHA* or *BRAVO* or *CHARLIE* or *DELTA*, from the least severe to the most (analogous to green, yellow, orange, and red depicting threat levels in the civilian sector such as airports). Unfortunately, one does not know how to numerically differentiate today's risk from yesterday's. If there was a numerical value, such as 90% security, one could tell just how secure we were thought to be, similar to the way one differentiated for temperature (Fahrenheit) readings. The same concept applies to the risk accrued for one's computer or a hospital's patient-centered healthcare system. To quantify and manage risk, the *RoM* tool based on a game-theoretic algorithm will be explained by citing examples.[29] The *RoM* method has been theoretically validated by Sahinoglu, Yuan, and Banks[32] through applying MAPLE software and through digital simulation as well.[29,30,61] This automated risk assessment and management algorithm provides a quantitatively strong alternative to the current mostly qualitative and subjective models. The model is explained below in four separate subsections for clarity.

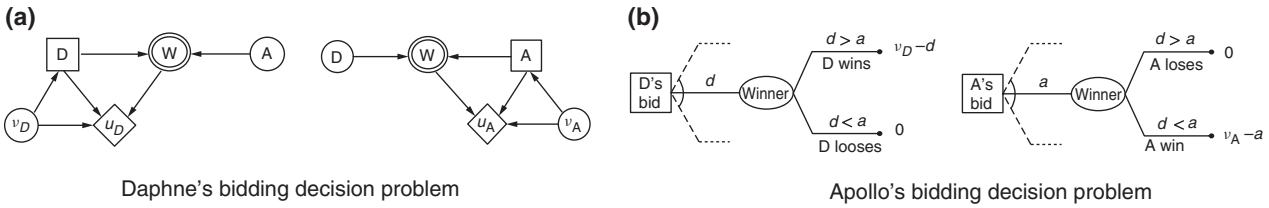


FIGURE 3 | Auction analysis from Daphne's and Apollo's bidding perspectives.

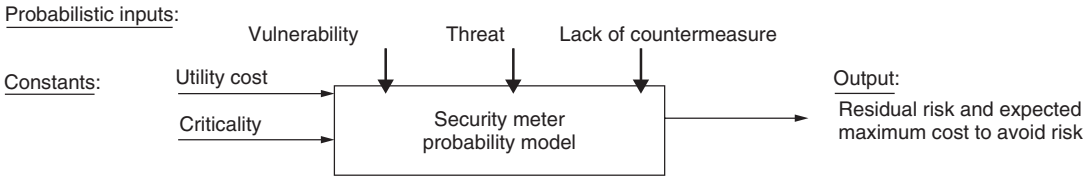


FIGURE 4 | Risk-O-Meter Model of probabilistic, deterministic inputs, and calculated outputs.

Probabilistic Inputs

The suggested vulnerability values vary between 0.0 and 1.0 (0 to 100%), adding up to one as cited in Figures 4 and 5. In a probabilistic sample space of feasible outcomes of the random variable of vulnerability or weakness, the sum of probabilities should add up to 1. This is like the probabilities of the faces of a die, such as 1–6, totaling to one. If a cited vulnerability is not exploited in reality, then it cannot be included in the model or simulation. Vulnerability has from one to several threats. A threat is defined as the probability of the exploitation of vulnerability within a specific time frame. Each threat has a countermeasure (*CM*) that ranges between 0 and 1 (with respect to the first law of probability) whose complement gives the *lack of countermeasure* (*LCM*). The binary *CM* and *LCM* values should add up to one, keeping in mind the second law of probability. The security risk analyst can define a network connectivity (v_1) as a vulnerability in which a threat (t_{11}), such as virus, or a hacker (t_{12}), could result in the destruction of software assets without countermeasures such as an antivirus (CM_{111}) or a firewall (CM_{121}), respectively.[29,30]

Deterministic Inputs

System criticality, a constant that indicates how critical or disruptive or consequential that a system is in the consequence of entire loss, is taken to be a single value ranging from 0.0 to 1.0 (0 to 100%) (see Figure 4). Criticality is low if residual risk is of little or no significance, such as a malfunctioning replaceable office printer. In the case of a nuclear power plant, or a patient undergoing a significant life and death surgery at a hospital, criticality would be close to a 100%, because RoS, *Risk of Service* has vital safety ramifications for irreplaceable lives and millions of dollars or more. Capital (*investment or utility*) *cost* is the total expected asset loss in monetary units (dollars, etc.) for a particular system if it is destroyed completely, and can no longer be utilized, excluding the other costs had the system continued to generate added value for the system. If there is an economic ripple or shadow-cost effect, a multiplier other than a default of unity (1.0) is needed.

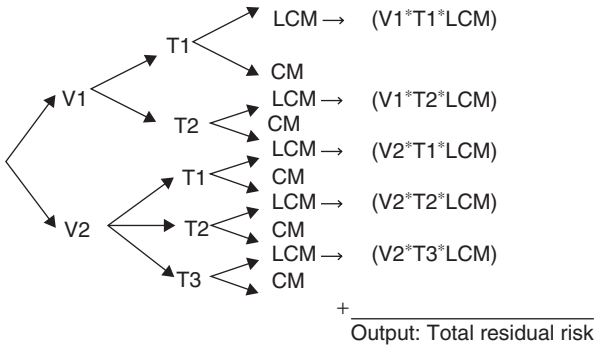


FIGURE 5 | General purpose tree diagram (V-branches, T-twigs, *LCM*-limbs) for the *RoM* model.

Probabilistic Tree Diagram

Given that a simple sample system or component has two or more outcomes for each risk factor, vulnerability, threat, and countermeasure, the following probabilistic framework holds for the sums $\sum v_i = 1$ and $\sum t_{ij} = 1$ for each i, and the sum of $LCM + CM = 1$ for each ij, within the tree diagram structure in Figure 5. Using the probabilistic inputs, we calculate the residual risk = vulnerability × threat × lack of countermeasure. We can calculate the residual risks for all vulnerabilities with threats and *LCM*s, as well as the total residual risk. That is, if we add all the residual risks due to the lack of countermeasures as in Figure 5, we can find the overall residual risk. We multiply the criticality factor with the residual risk to calculate the final risk. Then we apply the capital investment cost to the final risk to determine the expected cost of loss (*ECL*), which budgets for avoiding (before the attack) or repairing (after the attack) the entire risk where *ECL* ($) = final risk × capital cost.

Algorithmic Calculations

Figure 4 leads to a sample probabilistic tree diagram in Figure 5, which illustrates the calculations. For example, out of 100 malware attempts, the number of penetrating attacks not prevented will give the estimate of the percentage of *LCM*. One can then trace the root cause of the threat retrospectively in the tree diagram. In a cyber-security theme example: (1) a hacking network attack as a threat occurs; (2) the firewall software does not detect it; and (3) as a

result of this attack, whose root threat is known, the *network* as vulnerability is compromised. This example illustrates the *line of attack* on the tree diagram of Figure 5. Out of 100 such cyberattacks that maliciously harmed the target operation in any manner, how many of them were not countermeasured by, e.g., installed antivirus software or firewall? Out of those not prevented by a certain countermeasure (*CM*), how many of them were caused by threat 1 or 2, targeted for a particular vulnerability 1 or 2, etc.? Therefore, calculate for each limb in Figure 5, residual risk (*RR*) and sum the *RR*s for the total residual risk, *TRR*. Following the initial risk assessment, one proceeds with the risk management stage akin to *Price War example* in Section 2 to compute the game-theoretic linear programming solution vector CM_{ij} to mitigate risk from 26 to 10%. See Tables 7 and 8, using input in Table 6.

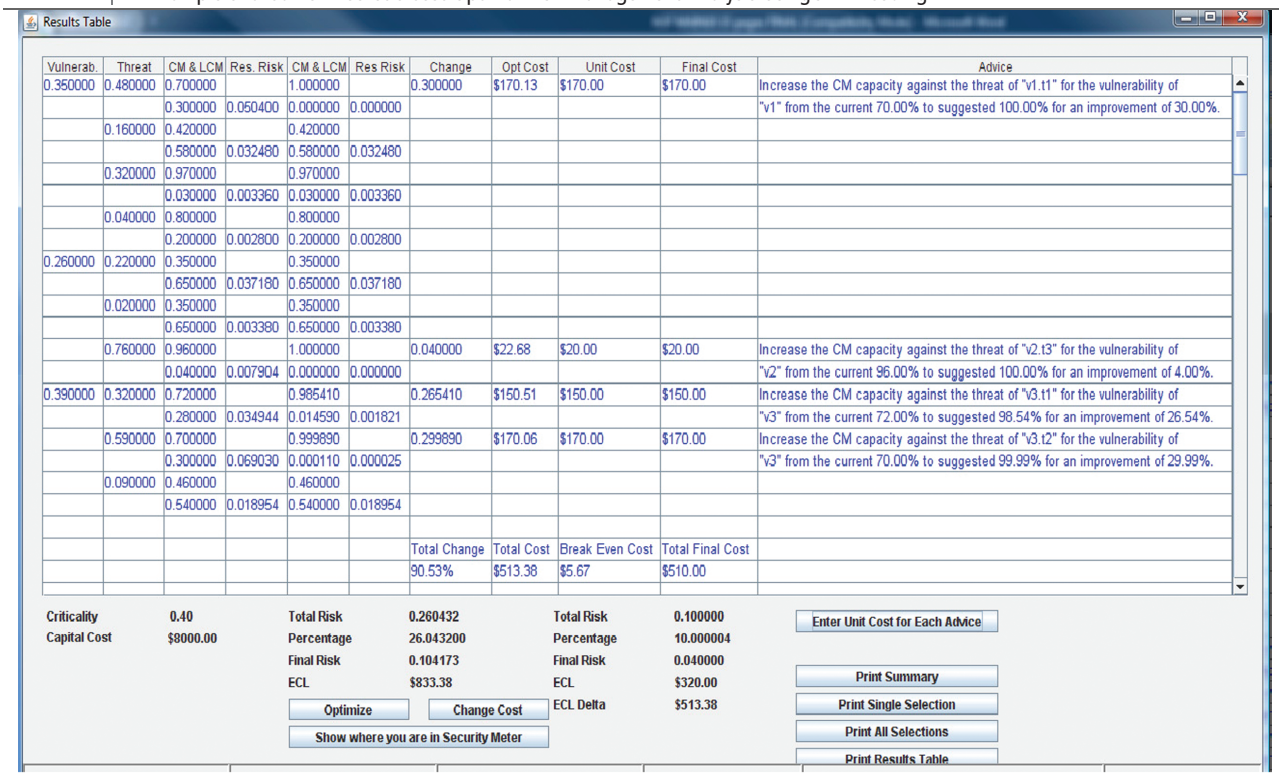
Expected Outcomes

Refer Table 7 for the risk management results regarding surveyed input data of Table 6.[30] After running the *RoM* through the software developed by the principal author, one obtains a break-even cost of $5.67 accrued per 1% countermeasure improvement. This is the result after the countermeasures are taken to bring the undesirable security risk (e.g., 26.04%) to a tolerable level (e.g., 10%). The average break-even cost *C* per 1% must be calculated to procure personnel, hardware, and software costs. On the positive side, the expected cost of loss (*ECL*) will decrease with a gain of ΔECL while the software and hardware etc. related *CM* improvements are added on. The break-even point is where the benefits and costs are equal, correctly guiding the security manager to follow up on corrective actions. The *Base Server* of the example in Table 7 (left half of Table 8) shows the organizational policy of mitigating the *RR* from 26.04% down to 10% (≤10%) in the *Improved Server*. Then for each improvement action, such as increasing from 70 to 100% for v_1t_1 branch etc., 30 × $5.67 = $170.1 is spent. The total minimal change of 90.52% × $5.6715 per 1% = $513.38 improvement cost, and ΔECL = $833.38 (base server) − $320 (improved server) = $513.38 for a diminished *RR* are now identical. Tables 7 and 8 show how the *RoM* is used to manage risk with a game-theoretic algorithm of threats versus countermeasures as two opposing actions. See Delta *ECL* of $513.38 at the bottom of Tables 7 and 8. If the user can find a provider to improve their PC or system for less than $5.67 per 1%, they will accrue a profit. Note, Table 7 (JAVA) or Table 8 (EXCEL) were built from a related security survey of a server at a U.S. University's Computer Center as illustrated

TABLE 6 | Sample Security Meter Input Probability Chart for a Local Server at a University Center[30]

Vulnerability	Threat	Countermeasure
$V_1 = 0.35$ (Internal Security Breach)	$T_{11} = 0.48$ (Internal Abuse of Network Access)	$CM_{11} = 0.70$ (Security Awareness Training) $LCM_{11} = 0.30$ by Subtraction
	$T_{12} = 0.16$ (System Penetration)	$CM_{12} = 0.42$ (Smart Cards) $LCM_{12} = 0.58$ by Subtraction
	$T_{13} = 0.32$ (Denial of Service)	$CM_{13} = 0.97$ (Firewalls) $LCM_{13} = 0.03$ by Subtraction
	$T_{14} = 0.04$ (Financial / Telecom Fraud)	$CM_{14} = 0.80$ (Security Audit) $LCM_{14} = 0.20$ by Subtraction
$V_2 = 0.26$ (External Security Breach)	$T_{21} = 0.22$ (Abuse of Wireless Network and Web Site Defacement)	$CM_{21} = 0.35$ (Public Key Infrastructure) $LCM_{21} = 0.65$ by Subtraction
	$T_{22} = 0.02$ (Sabotage)	$CM_{22} = 0.35$ (Intrusion Prevention) $LCM_{22} = 0.65$ by Subtraction
	$T_{23} = 0.76$ (Virus)	$CM_{23} = 0.96$ (Anti -Virus) $LCM_{23} = 0.04$ by Subtraction
$V_3 = 0.39$ (Both Internal and External Breach)	$T_{31} = 0.32$ (Unauthorized Info Access)	$CM_{31} = 0.72$ (Intrusion Detection) $LCM_{31} = 0.28$ by Subtraction
	$T_{32} = 0.59$ (Malicious Code)	$CM_{32} = 0.70$ (Server Access) $LCM_{32} = 0.30$ by Subtraction
	$T_{33} = 0.09$ (Theft of Proprietary Information)	$CM_{33} = 0.46$ (Encrypted Files) $LCM_{33} = 0.54$ by Subtraction

TABLE 7 | An Example of a Game-Theoretic Cost-Optimal Risk Management Analysis Using JAVA Coding



Results Table

Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.350000	0.480000	0.700000		1.000000		0.300000	$170.13	$170.00	$170.00	Increase the CM capacity against the threat of "v1.t1" for the vulnerability of
		0.300000	0.050400	0.000000	0.000000					"v1" from the current 70.00% to suggested 100.00% for an improvement of 30.00%.
	0.160000	0.420000		0.420000						
		0.580000	0.032480	0.580000	0.032480					
	0.320000	0.970000		0.970000						
		0.030000	0.003360	0.030000	0.003360					
	0.040000	0.800000		0.800000						
		0.200000	0.002800	0.200000	0.002800					
0.260000	0.220000	0.350000		0.350000						
		0.650000	0.037180	0.650000	0.037180					
	0.020000	0.350000		0.350000						
		0.650000	0.003380	0.650000	0.003380					
	0.760000	0.960000		1.000000		0.040000	$22.68	$20.00	$20.00	Increase the CM capacity against the threat of "v2.t3" for the vulnerability of
		0.040000	0.007904	0.000000	0.000000					"v2" from the current 96.00% to suggested 100.00% for an improvement of 4.00%.
0.390000	0.320000	0.720000		0.985410		0.265410	$150.51	$150.00	$150.00	Increase the CM capacity against the threat of "v3.t1" for the vulnerability of
		0.280000	0.034944	0.014590	0.001821					"v3" from the current 72.00% to suggested 98.54% for an improvement of 26.54%.
	0.590000	0.700000		0.999890		0.299890	$170.06	$170.00	$170.00	Increase the CM capacity against the threat of "v3.t2" for the vulnerability of
		0.300000	0.069030	0.000110	0.000025					"v3" from the current 70.00% to suggested 99.99% for an improvement of 29.99%.
	0.090000	0.460000		0.460000						
		0.540000	0.018954	0.540000	0.018954					
						Total Change	Total Cost	Break Even Cost	Total Final Cost	
						90.53%	$513.38	$5.67	$510.00	

Criticality 0.40 | Capital Cost $8000.00 | Total Risk 0.260432 | Percentage 26.043200 | Final Risk 0.104173 | ECL $833.38 | Total Risk 0.100000 | Percentage 10.000004 | Final Risk 0.040000 | ECL $320.00 | ECL Delta $513.38

Optimize | Change Cost | Show where you are in Security Meter | Enter Unit Cost for Each Advice | Print Summary | Print Single Selection | Print All Selections | Print Results Table

in Table 6.[30] Consequently, optimal countermeasures are generated using a game-theoretic computational algorithm, *RoM*, to optimize mitigation as illustrated under the *Change* column. The algorithm brings significant advantages to information warfare[22,23,30,61] on how to optimize the countermeasures (*CM*) in an offense versus defense setting in national cybersecurity theme.[62,63]

Clarifications for RoM Results in Tables 6–10 for the Production Server at a University Center

Using the input chart of Table 6 and the results of Tables 7 and 8 and to improve the base risk by mitigating from 26 to 10%, we implement the prioritized and recommended actions from the *Advice* column as follow: (1) Increase the *CM* capacity for the vulnerability of *Internal Security Breach* and its threat *Internal Abuse of Network Access* from the current 70 to 100%. (2) Increase the *CM* capacity for the vulnerability of *External Security Breach* and its threat *Virus* from the current 96 to 100%. (3) Increase the *CM* capacity for the vulnerability of *Both Internal and External Breach* and its threat *Unauthorized Info Access* from the current 72 to 98.54%. (4) Increase the *CM* capacity for the vulnerability of *Both Internal and External Breach* and its threat *Malicious Code* from the current 70 to 99.99%. In pursuing these actions, as in Table 7, a *Total Final Cost* of $510 is dispensed (<$513.38 as advised) each within the limits of optimal costs annotated, staying below the break-even cost of $5.67 per every %*CM* improvement. The next management step may proceed with seeking optimization to a next desirable percentage once these *CM* services are provided, such as mitigating to 5 from 10% if the budget exists. One can also see under Table 8's *Game* column 11, the alternative *CM* values were obtained through a new LP optimal solution in Table 9 where the *improvement* constraint, i.e., ≥column 3 is liberated or disabled. Namely, the *CM* constraints earlier in column 5 for the sought optimal vector were bound to be greater than or equal (≥) to those previously enabled in column 3 for improvement. The new solution CM vector as in column 11 all may not be ≥ those of column 3 as one can see in Table 8's *Change* column 10 that may contain a negative value (red). For this alternative in Table 9, to provide the same benefits, one has to experience a change of 310.9% at the bottom of column 10 compared to 90.5% of column 7 in Table 8. Then, for a fixed cost of recovery, one has to pay at least three times. However, columns 8 and 13 of Table 8 yield the identical *ECL* (expected cost of loss) due to differing break-even costs. Therefore,

TABLE 8 | An Example of Game-Theoretic Cost-Optimal Risk Management (Mixed Strategy using EXCEL)

1	2	3	4	5	6	7	8	9	10	11	12	13
Vuln	Threat	CM & LCM	Res. Risk	CM & LCM	Res. Risk	Change	Cost	Beta M'lier	Change	Game	BetaVector	NE COST
0.35	0.48	0.7		1		0.3	$170.14	0.3333333	0.284	0.98	0.01654	$46.88
		0.3	0.0504	0	0							
	0.16	0.42		0.42		0	$0.00	1	0.58	1	0.04962	$95.78
		0.58	0.03248	0.58	0.03248							
	0.32	0.97		0.97		0	$0.00	0.5	0.03	1	0.02481	$4.95
		0.03	0.00336	0.03	0.00336							
	0.04	0.8		0.8		0	$0.00	4	0.2	1	0.19849	$33.03
		0.2	0.0028	0.2	0.0028							
0.26	0.22	0.35		0.35		0	$0.00	0.979021	0.65	1	0.04858	$107.34
		0.65	0.03718	0.65	0.03718							
	0.02	0.35		0.35		0	$0.00	10.769231	0.65	1	0.53439	$107.34
		0.65	0.00338	0.65	0.00338							
	0.76	0.96		1		0.04	$22.69	0.2834008	-0.124	0.84	0.01406	-$20.39
		0.04	0.007904	0	0							
0.39	0.32	0.72		0.9852		0.2652	$150.41	0.4487179	0.28	1	0.02227	$46.24
		0.28	0.034944	0.0148	0.00185							
	0.59	0.7		1		0.3	$170.14	0.2433724	0.018	0.72	0.01208	$3.04
		0.3	0.06903	0	0							
	0.09	0.46		0.46		0	$0.00	1.5954416	0.54	1	0.07917	$89.17
		0.54	0.018954	0.54	0.01895			M'lierSum	Total=			CostSum=
	SUMnew	Total Risk	0.260432	Tot RISK	0.1	0.9052	$513.38	20.152518	3.109		BetaTotal=	$513.38
	7.3352	Percentage	26.04%	Percentage	10.00%			Beta Sub2=			1	
BASE	SERVER	Final Risk	0.104173	Final Risk	0.04	IMPRVD	SERVER	0.0496216			NESolution	NE TotCmij=
Asset=	$8000	ECL	$833.38	ECL	$320.00			Total CMij			0.17868	3.34
Criticality=	0.40	Total CMij	6.43	Delta ECL	$513.38	per%		$5.67	6.43	$1.65	17.87%	

TABLE 9 | LP Solution of Example of Tables 6–8 When $\geq$ Constraints not Placed on CM_{ij} in Column 3 of Table 8

Optimal Solution
Objective Function Value = 0.1653

Variable	Value	Reduced Costs
X1	0.9839	0.0000
X2	1.0000	0.0000
X3	1.0000	0.0000
X4	1.0000	0.0000
X5	1.0000	0.0000
X6	1.0000	0.0000
X7	0.8365	0.0000
X8	1.0000	0.0000
X9	0.7184	0.0000
X10	1.0000	0.0000
X11	0.1653	0.0000

what's in *Change* column of Table 7 (JAVA) that is identical to column 7 of Table 8 (EXCEL) is the most optimal solution. Column 10 is the difference vector between column 11 (an alternative mixed strategy solution using Table 9 LP solution when the greater than or equal to column 3's countermeasures are omitted for free ride solution) and column 3 of CM_{ij} also in Table 10 through Table 6. *Defense* (user) picks the smallest column-wise, while *Offense* (attacker) picks the largest row-wise risk. This is how the Maximin = Minimax works as in Table 10 illustrating the diagonal loss matrix.

TABLE 10 | Diagonal Loss Matrix of Table 8 (Columns 1–3, 5) of Neumann Mixed Strategy and β(Column 12) of Nash Mixed Strategy

	CM_{11} = 0.70, β_1 = 0.01652	CM_{12} = 0.42, β_2 = 0.04962	CM_{13} = 0.97, β_3 = 0.02481	CM_{14} = 0.80, β_4 = 0.19849	CM_{21} = 0.35, β_5 = 0.04859	CM_{22} = 0.35, β_6 = 0.053439	CM_{23} = 0.96, β_7 = 0.01406	CM_{31} = 0.72, β_8 = 0.02227	CM_{32} = 0.70, β_9 = 0.01208	CM_{33} = 0.46, β_{10} = 0.07917
$V_1 \times T_{11}$ = 0.35 × 0.48	0.168									
$V_1 \times T_{12}$ = 0.35 × 0.16		0.056								
$V_1 \times T_{13}$ = 0.35 × 0.32			0.112							
$V_1 \times T_{14}$ = 0.35 × 0.04				0.014						
$V_2 \times T_{21}$ = 0.26 × 0.22					0.0572					
$V_2 \times T_{22}$ = 0.26 × 0.02						0.0052 Minimax				
$V_2 \times T_{23}$ = 0.26 × 0.76							0.1976			
$V_3 \times T_{31}$ = 0.39 × 0.32								0.1248		
$V_3 \times T_{32}$ = 0.39 × 0.59									0.2301 Maximin	
$V_3 \times T_{33}$ = 0.39 × 0.09										0.0351

Other Interdisciplinary Applications of RoM

The *RoM*'s risk assessor and manager expert system is capable of implementing this algorithm into diverse themes such as[62–68]:

1. Computer and Network Security Risk-O-Meter
2. Computer and Network (including Social Networks) Privacy/Security Risk-O-Meter
3. Ecological Risk-O-Meter
4. Electronic-Voting Risk-O-Meter
5. Business Contract Risk-O-Meter
6. Campus Safety and Security Risk-O-Meter
7. Department of Public Health HIPAA (Privacy/Security) Risk-O-Meter
8. Hospital-Based Non-Ambulatory Patient-Centered Healthcare Risk-O-Meter
9. National and State Cyber-Security Risk-O-Meter
10. Federal Cyber-Security Risk-O-Meter
11. Mining Safety and Security Risk-O-Meter
12. Off-Shore Oil-Spill Wireless Sensory Network (WSN) Risk-O-Meter
13. Usability Risk-O-Meter
14. Cloud Risk-O-Meter
15. Airport Service Risk-O-Meter.

For the sake of a popular example, let us present a case in regards to the item 2 (Social Networks Privacy/Security Risk-O-Meter) from the listing above, where a number of real people (not simulated) were interviewed and the results were discussed.[67] With the advent and unprecedented popularity of the now ubiquitous social networking sites such as Google+, Facebook, MySpace, and Twitter etc. in the personal sphere and others such as LinkedIn in business circles, undesirable security, and privacy risk issues have come to the forefront as a result of this extraordinary rapid growth. The most salient issues are mainly lack of trustworthiness; namely, those of security and privacy.

One can address these issues by employing a quantitative approach to assess security and privacy risks for social networks already under pressure by users and policymakers for breaches in both quality and sustainability. One can also demonstrate, using a cost-optimal game-theoretic solution using *RoM* algorithmic tool, how to assess and manage risk. The applicability of this research to diverse fields from security to privacy and health care, and eco-risk or business is an additional asset. See section on *Social Networks Privacy/Security Risk-O-Meter Example* on the social networks' privacy/security theme along with both Neumann and Nash mixed strategy solutions.

Application of Nash Equilibrium Mixed Strategy Solution to Risk-O-Meter Assessment and Management

University Server's Security Risk-O-Meter Example

In the preceding university server's security example of Tables 6–9 applying *RoM*, we had a strictly diagonal loss (opposite to utility or payoff) matrix. The probabilistic action set is not discrete but continuous and differentiable, and all lie between 0 and 1. Note CM_{ij} in the *CM* and *LCM* column in Tables 7, 8, and 10. Let us start with differentiating diagonal matrix's *expected loss* in Table 10, such as in Section on *Games with Multiple Nash Equilibria (Terrorist Game: Bold Strategy Can Result in Domination)*, to obtain the NE solution vector. See Eq. (3–8).

$$\begin{aligned}\Pi_C = {} & (1-0.168)\alpha_1\beta_1 + (1-0.056)\alpha_2\beta_2 \\ & + (1-0.112)\alpha_3\beta_3 + (1-0.014)\alpha_4\beta_4 \\ & + (1-0.0572)\alpha_5\beta_5 + (1-0.0052)\alpha_6\beta_6 \\ & + (1-0.1976)\alpha_7\beta_7 + (1-0.1248)\alpha_8\beta_8 \\ & + (1-0.2301)\alpha_9\beta_9 + (1-0.0351) \\ & \times ((1-\alpha_1-\alpha_2-\alpha_3-\alpha_4-\alpha_5-\alpha_6 \\ & - \alpha_7-\alpha_8-\alpha_9)(1-\beta_1-\beta_2-\beta_3-\beta_4 \\ & - \beta_5-\beta_6-\beta_7-\beta_8-\beta_9)) \qquad (3)\end{aligned}$$

Then, the Nash equilibrium $(\alpha\beta)^T$ vector can be obtained by solving the simultaneous differentiable equations $\frac{\partial \Pi_C}{\partial \alpha}$ and $\frac{\partial \Pi_C}{\partial \beta}$ for α and β vectors that are continuous variables defined in (0,1).[57,64,68]

Taking the derivatives and equating to zero:

$$\frac{\partial \Pi_C}{\partial \alpha_1} = 0.168\beta_1 - 0.0351\left(1 - \sum_{i=1}^{9}\beta_i\right) = 0 \qquad (4)$$

$$\frac{\partial \Pi_C}{\partial \alpha_2} = 0.056\beta_2 - 0.0351\left(1 - \sum_{i=1}^{9}\beta_i\right) = 0 \qquad (5)$$

. . . . . .

$$\frac{\partial \Pi_C}{\partial \alpha_9} = 0.2301\beta_9 - 0.0351\left(1 - \sum_{i=1}^{9}\beta_i\right) = 0 \qquad (6)$$

Therefore, the resultant equations for the Nash equilibrium's differential equations are given as follows:

$$0.168\beta_1 = 0.056\beta_2 \rightarrow \beta_1 = 0.333\beta_2$$

$$0.056\beta_2 = 0.112\beta_3 \rightarrow \beta_3 = 0.500\beta_2$$

$$\begin{aligned}0.112\beta_3 &= 0.014\beta_4 \rightarrow \beta_4 = 4\beta_2 \\ 0.014\beta_4 &= 0.0572\beta_5 \rightarrow \beta_5 = 0.9792075\beta_2 \\ 0.0572\beta_5 &= 0.0052\beta_6 \rightarrow \beta_6 = 10.769229\beta_2 \\ 0.0052\beta_6 &= 0.1976\beta_7 \rightarrow \beta_7 = 0.283403\beta_2 \\ 0.1976\beta_7 &= 0.1248\beta_8 \rightarrow \beta_8 = 0.448721\beta_2 \\ 0.1248\beta_8 &= 0.2301\beta_9 \rightarrow \beta_9 = 0.243374\beta_2 \\ 0.2301\beta_9 &= 0.0351\beta_{10} \rightarrow \beta_{10} = 1.595454\beta_2 \qquad (7)\end{aligned}$$

Also, $\beta_2 = 1.0\beta_2$ (identity). Now add $\sum \beta_i = 20.1524\ \beta_2 = 1.000 \rightarrow \beta_2 = 0.049622$.

Final Nash equilibrium solution vector for β_i (substituting in Eq. (7) as tabulated in Table 10 is as follows:

$$\begin{aligned}\beta_1 &= 0.0165241 \\ \beta_2 &= 0.0496218 \\ \beta_3 &= 0.0248109 \\ \beta_4 &= 0.1984872 \\ \beta_5 &= 0.0485900 \\ \beta_6 &= 0.5343885 \\ \beta_7 &= 0.0140629 \\ \beta_8 &= 0.0222663 \\ \beta_9 &= 0.0120766 \\ \beta_{10} &= 0.0791693 \qquad (8)\end{aligned}$$

Now add $\sum \beta_i = 1.000$, which checks to unity.

Also $\alpha_i = \beta_i$, for $i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. Therefore, there is no need to solve $\frac{\partial \Pi_C}{\partial \alpha}$.

These β multipliers of Eq. (7) are displayed under *Beta M'lier* in column 9 of Table 8, where $\beta_2 = 0.049622$. The final Nash equilibrium's *Beta Vector* is displayed in column 12 of Table 8, as well as Table 10's top row, summing to β total = 1.00. If this solution vector is unconstrained and used as is, the residual risk will fall to 17.87% as shown at the bottom of column 12 from an original 26.04% in column 4. However, some of these NE solution vector values are infeasible since they exceed a probability of 1.00, such as in the case of $\beta_6 = 0.534$, which actually means $CM_{22} = 0.534 \times 6.43$ (countermeasures summed total CM_{ij} at the bottom of column 4 in Table 8) = 3.43 > 1.0. This cannot to be allowed since CM_{ij} probabilities cannot exceed 1.0. Therefore, the NE solution vector is not valid. We review a diagonal matrix case as in Table 11. NE solution is feasible, but engineering-wise not realistic.

TABLE 11 | Social Network Privacy/Security Risk Example Using Cost-Optimal Risk Analysis with ***RoM***

Social Networks Privacy/Security Risk-o-Meter Example

In another example, see Table 11 for the application of NE solutions on a new *RoM* scenario. In a new example seeking NE solution vector for the *RoM* tableau in Table 11 for a different problem from Ref 67, the *RoM*'s CM_{ij} solution vector is obtained as follows with respect to Table 11. Solving the differential equations for the NE vector through Eqs (9) and (10) as we did in the previous example, the NE mixed strategy solution vector is

$$\begin{aligned}
0.1078\beta_1 = 0.1862\beta_2 &\rightarrow \beta_1 = 1.727\beta_2 \\
0.1862\beta_2 = 0.076\beta_3 &\rightarrow \beta_3 = 2.45\beta_2 \\
0.076\beta_3 = 0.117\beta_4 &\rightarrow \beta_4 = 1.591\beta_2 \\
0.117\beta_4 = 0.09\beta_5 &\rightarrow \beta_5 = 2.069\beta_2 \\
0.09\beta_5 = 0.093\beta_6 &\rightarrow \beta_6 = 2.002\beta_2 \\
0.093\beta_6 = 0.1176\beta_7 &\rightarrow \beta_7 = 1.582\beta_2 \\
0.1176\beta_7 = 0.0924\beta_8 &\rightarrow \beta_8 = 2.015\beta_2 \qquad (9)
\end{aligned}$$

Also, $\beta_2 = 1.0\beta_2$ (identity). Now add $\sum \beta_i = 14.43\ \beta_2 = 1.000 \rightarrow \beta_2 = 0.069278$.

Final Nash equilibrium mixed strategy solution vector for β_i:

$$\begin{aligned}
\beta_1 = 0.119644 &\rightarrow \beta_1\ x\ 5.06 = 0.61 = CM_{11} \\
\beta_2 = 0.069278 &\rightarrow \beta_2\ x\ 5.06 = 0.35 = CM_{12} \\
\beta_3 = 0.169732 &\rightarrow \beta_3\ x\ 5.06 = 0.86 = CM_{13} \\
\beta_4 = 0.110222 &\rightarrow \beta_4\ x\ 5.06 = 0.56 = CM_{21} \\
\beta_5 = 0.143337 &\rightarrow \beta_5\ x\ 5.06 = 0.73 = CM_{22} \\
\beta_6 = 0.138695 &\rightarrow \beta_6\ x\ 5.06 = 0.70 = CM_{23} \\
\beta_7 = 0.109598 &\rightarrow \beta_7\ x\ 5.06 = 0.55 = CM_{31} \\
\beta_8 = 0.139596 &\rightarrow \beta_8\ x\ 5.06 = 0.71 = CM_{32} \qquad (10)
\end{aligned}$$

Now add $\sum \beta_i = 1.000$ which checks. Also $\beta_i = \alpha_i$, for $i = 1, 2, 3, 4, 5, 6, 7, 8$. Also $\alpha_i = \beta_i$, *for* $i = j$.

CM_{ij} sum $= 0.53 + 0.85 + 0.69 + 0.63 + 0.73 + 0.6 + 0.5 + 0.53 = 5.06$, by adding column 3 (*CM* and *LCM*) in Table 11.

When calculated, although feasible, NE vector worsened risk level from 34.5 to 37.5% (while a mitigation drop was expected), i.e., when these NE vector values are implemented as we did in Table 8. From Table 11, $TRR = 1 - \sum_{i,j,k} V_i T_j CM_{ijk} = 1 - 0.493506 \times [0.218599 \times 0.61 + 0.379831 \times 0.35 + 0.401570 \times 0.86] - 0.298701 \times [0.385572 \times 0.56 + 0.298507 \times 0.73 + 0.315920 \times 0.70] - 0.207792 \times [0.558389 \times 0.55 + 0.441611 \times 0.71] = 1 - 0.0653 + 0.0651 + 0.1702 + 0.0642 + 0.0647 + 0.0662 + 0.0644 + 0.0646 = 1 - 0.625 = 0.375$. Although NE solution computationally worked, it is not practical because new CM_{ij} do not mitigate risk!

Clarification of Risk Assessment and Management Algorithm (RoM) Using Figure 6 and Table 11

To mitigate a certain survey taker's (representing an undisclosed identity with a median risk value of 34.5% amidst nine graduate students randomly selected from social network users at an international University, METU, Ankara, Turkey) social network privacy/security risk from 34.5 to 24%, following countermeasures (*CM*) were guided by the *RoM* as follows[67]: (1) Increase the *CM* capacity for the threat of *E-Mail hijacking* in the vulnerability of *Correspondence* from 85 to 100% for an improvement of 15% by procuring goods or services for $210.93. (2) Increase the *CM* capacity for the threat of *E-Commerce* in the vulnerability of *Correspondence* from 69.5 to 100% for an improvement of 30.50% by procuring goods or services for $428.84. (3) Increase the *CM* capacity for the threat of *Easily Guessed Passwords* in the vulnerability of *Password* from 50 to 64.36% for an improvement of 14.36% by procuring goods or services for $201.99.

A total cost of $841.76 is allocated to mitigate the risk from 34.5 to 24% for cost-optimal improvement yielding a *Total Change* of 59.86% as *RoM* results show in Table 11. She/he can recursively continue to mitigate the present risk of 24% (down from an initial 34.5%) to lower target values such as 10% if she/he has a sufficient budget remaining for further improvement. This is to say that she/he (median survey taker) will implement the above-clarified countermeasures by purchasing the services needed to mitigate her/his privacy/security risk from a high of 34.5% to a low of 24%. She/he will do that by simply referring to the *CM* questions as cited, and converting the negative (No) responses to positives (Yes) by taking recommended countermeasures. While doing so, she/he will optimize her/his costs by following the optimal allocation plan suggested by the *RoM*'s game-theoretical solutions, which are Neumann mixed strategy. NE mixed strategy solution did not generate an improvement on 34.5%, conversely worsening to 37.5%. Utility or asset of $8000 was assumed, see Figure 4.

CONCLUSIONS, DISCUSSIONS, AND FUTURE RESEARCH

Although Game theory from its inception is almost 150 years old, it started gaining prevalence and worldwide recognition around the end of the Second World War when decisions regarding newly introduced nuclear weapons meant possible life or death for mankind. Game theory-related computing began first in 1944 along with Dantzig's breakthrough on simplex method with Neumann and Morgenstern's pioneering book.[3] Nash brought a reconciliatory flavor to Neumann's WW2 era findings within an economic context in 1950.[5] Since the advent of Internet connectivity in 1990s and the exponential rise of correspondence and malicious malware without borders, game theory is viewed as a tool for protecting ubiquitous Cybersystems and Information Security against enemies and adversaries, which operate both in rational and irrational modes. It is anticipated that cyber-armies will replace conventional forces with cyberspace command needing more resources than warplanes or submarines in the next decades. Scanning a history of 150 years, this review delves into computationally intensive methods to show why and how game-theoretic risk analysis works from statistical, business, and engineering viewpoints to name a few. Major examples are illustrated to highlight the significance of these methods, i.e., from Neumann's two-way zero-sum to those of mixed strategy, and moreover Nash equilibrium while citing computational and theoretical difficulties and solutions. An example of adversarial risk analysis (ARA) by other scientists is also illustrated. Nowadays, game theory is not dichotomous as it used to be, such as Neumann versus Nash methods, but multifaceted. The new game theoreticians, e.g., Aumann and Banks[19,38,39] are exploring critiques in search of new techniques since the nature of players has changed from rational to irrational, and erratic or terrorist. Moreover, Sahinoglu's Risk-o-Meter[29,30,61] technique is reviewed through pure and mixed strategy solutions from Neumann and Nash Equilibria viewpoints. This has led to a quantitative risk assessment and mitigation software tool, scalable and applicable into daily practice for diversely popular disciplines.[61–68]

In summary, therefore, following an informative introduction to gaming and origins in Section *Introduction to Gaming and Historical Perspective to Game Theory's Origin*, a technical background with conceptual definitions supported by numerical examples is presented in Section *Intuitive Background—Concepts, Definitions, and Nomenclature of Game Theory*. In Section *Random Probabilistic Selection for Nash Mixed Strategy Equilibria—Various Scenarios*, more in-depth Nash nomenclature and solutions are studied citing scenarios from the literature. Certain ARA models are reviewed in Section *Adversarial Risk Analysis (ARA) Models* with certain illustrations from their proponents. Regarding an alternative probabilistic risk assessment and cost-optimal game-theoretic management algorithm, i.e., Risk-o-Meter (*RoM*); various examples of Neumann's

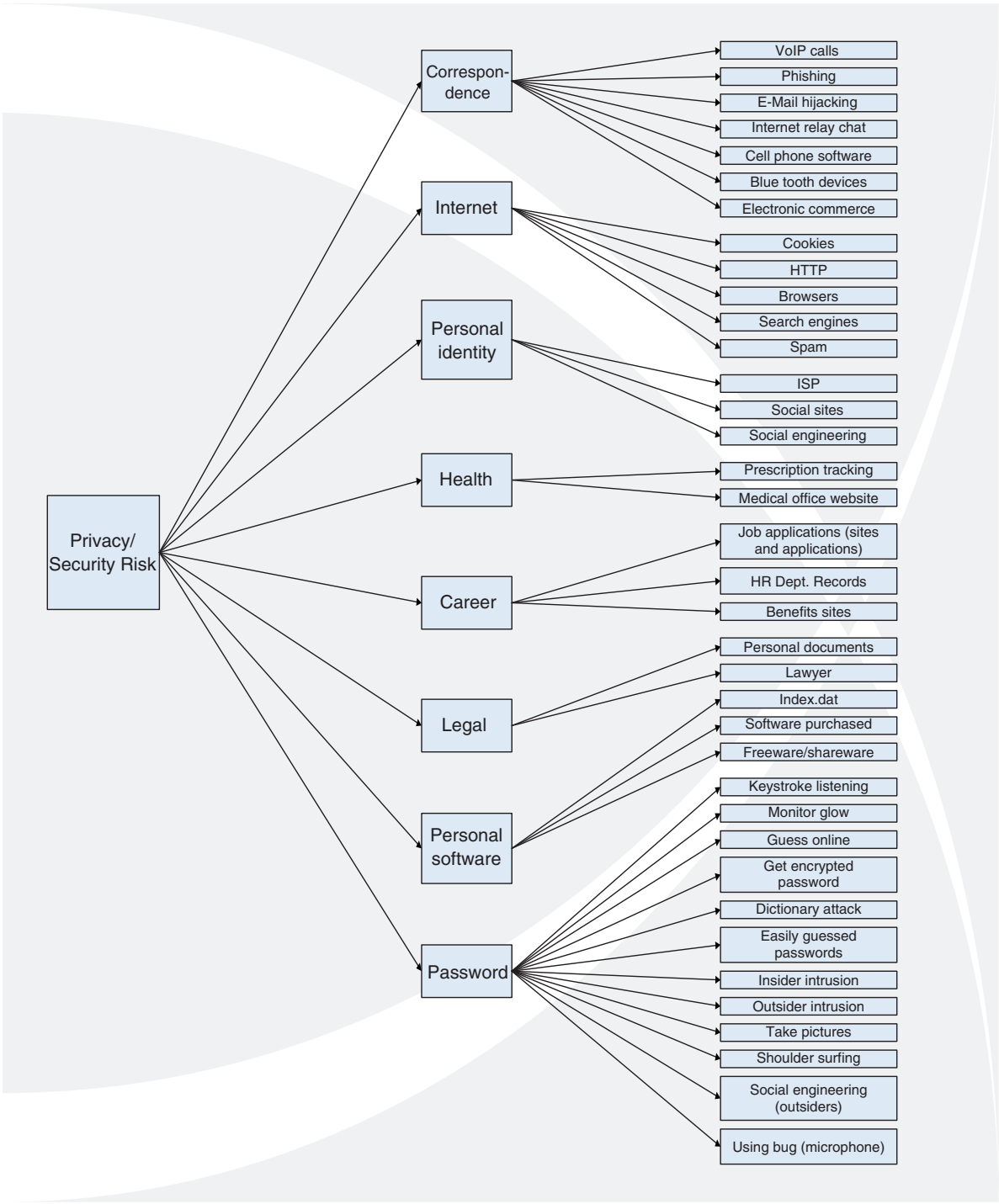


FIGURE 6 | An example for social network privacy/security risk-o-meter tree diagram using *RoM*.

and Nash equilibrium solutions in Sections *Neumann's Mixed Strategy Solutions to Risk-O-Meter (RoM) Assessment and Management Algorithm* and *Application of Nash Equilibrium Mixed Strategy Solution to Risk-O-Meter Assessment and Management*, with respect to engineering realities and probabilistic laws are also reviewed. Nash solutions are shown to demonstrate a complete consensus between the elements of the defense (good) and offense (hostile). Whatever one player challenges, the rival player concurs with, leading to a complete agreement status in effect minimizing the damage or maximizes the

gain from whatever angle one views it. This is evident from the identical Eqs 4–6, 9–10 in Section *Alternative Model: Sahinoglu's Security Meter (Risk-O-Meter) for Game-Theoretic Applications to Assess and Manage Risk By mixed Strategy Using Neumann and Nash Equilibria*. However, the reality is quite different from this idealistic scenario, since terrorists and defenders do not simply concur to be kind out of courtesy. This review displays only a non-exhaustive selection of predominant games, with recent alternative game solutions. There may be many solution genres of game theory as there are problems. Game-theoretic computing topics in risk analysis have recently become important elements of course syllabi taught at cybersecurity degree programs such as in the Cybersystems and Information Security (CSIS) graduate degree program at Auburn University Montgomery (www.aum.edu/csis).[69] The future of game-theoretic computing lies in not only deriving smart novel models but also articulating them for the layman or potential industrial user or risk analyst, by demonstrating how to apply them in an algorithmic order through crunching real-life data and obtaining meaningful solutions to interpret. Scope of future research entails overriding some of the limitations of the status-quo game-theoretic practices, which include idealized scenarios [[21]p. 7; [24]p. 12].

REFERENCES

1. Shubik M. *Games for Society, Business and War: Towards a Theory of Gaming*. New York: Elsevier; 1975.
2. Rapaport A. *Two-Person Game Theory: The Essential Ideas*. Ann Arbor: University of Michigan Press; 1966.
3. Neumann JV, Morgenstern O. *Theory of Games and Economic Behavior*. Princeton: Princeton University Press; 1944.
4. Glicksman AM. *Linear Programming and the Theory of Games*. New York and London: John Wiley & Sons Inc.; 1963.
5. Nash JF. Equilibrium points in N-Person games. *Proc Natl Acad Sci U S A* 1950, 36:48–49.
6. Cournot A. In: Bacon, N., ed. *Recherches Sur Les Principes Mathematiques De La Theorie Des Richesses (Researches into the Mathematical Principles of the Theory of Wealth)*. English edition. New York: Macmillan; 1897.
7. Bertrand J. Theorie mathematique de la richesse social. *J Savants* 1883, 48:499–508.
8. Edgeworth FY. La Teoria pura del monopolio. *Giornale degli Economisti* 1897, 11:13–31.
9. Stigler SM. Francis Ysidro Edgeworth, Statistician (with discussion). *J R Stat Soc [Ser A]* 1978, 141:287–322.
10. Selten R. Spieltheoretishe behandlung eines oligopol-models mit nachfragetragheit. *Z Gesamte Statswiss* 1965, 12:301–324.
11. Selten R. A re-examination of the perfectness concept for equilibrium points in extensive games. *Int J Game Theory* 1975, 4:25–55.
12. Harsanyi JC. Games with incomplete information played by Bayesian players. Parts I, II, III. *Manag Sci* 1967, 14:159–182, 320–334, 486–502.
13. Fudenberg D, Tirole J. *Game Theory*. Cambridge, MA: MIT Press; 1991.
14. Osborne MJ. *An Introduction to Game Theory*. New York, NY: Oxford University Press; 2004.
15. Osborne MJ, Rubinstein, A. *A Course in Game Theory*. Cambridge, MA: MIT Press; 1994.
16. Binmore KG. *Does Game Theory Work*. Cambridge, MA: MIT Press; 2007.
17. Morton DD. *Game Theory: A Nontechnical Introduction*. New York: Basic Books Inc. Publishers; 1970.
18. Jones AJ. *Game Theory: Mathematical Models of Conflict*. Chichester: Ellis Horwood Limited; 1980.
19. Aumann R, Dreze J. Rational expectations in games. *Am Econ Rev* 2008, 98:72–86. Available at: http://www.ma.huji.\penalty\@Mac.il/raumann/pdf/86.pdf. (Accessed 2010).
20. Kadane JB, Larkey PD. Subjective probability and the theory of games. *Manag Sci* 1982, 28:113–120.
21. Roy SE, Shiva S, Dasgupta D, Shandilya V, Wu Q. A survey of game theory as applied to network security. *Proceedings 43rd Hawaii International Conference on System Sciences (HICSS)*; 2010, 1–10.
22. Hamilton SN, Miller WL, Ott A, Saydjari OS. Challenges in applying game theory to the domain of information warfare. *Proceedings of the 4th Information Survivability Workshop*. 2002, ISW 2001/2002, Vancouver, Canada.
23. Hamilton SN, Miller WL, Ott A, Saydjari OS. The role of game theory in information warfare. *Proceedings of the 4th Information Survivability Workshop*, 2002, ISW 2001/2002, Vancouver, Canada.
24. Lye KW, Wing J. Game strategies in network security. CMU-CS-02-136(DARPA and ARO Contract No. DAAD19-01- 1-0485), *Proceedings of the Foundations of Computer Security*, Copenhagen, Denmark, 2002.
25. Lye KW, Wing J. Game strategies in network security. *Int J Inf Sec* 2005, 4:71–86.

26. Cavusoglu H, Mishra B, Raghunatan S. A model for evaluating IT security investments. *Commun ACM* 2004, 47:87–92.
27. Patcha A, Park J. A game theoretic approach to modeling intrusion detection in mobile and ad hoc networks. *Proceedings of the 2004 IEEE Workshop on Information Assurance and Security*. West Point, NY: United States Military Academy; 2004.
28. Jormakka J, Mölsä JVE. Modeling information warfare as a game. *J Inf Warf* 2005, 4:12–25.
29. Sahinoglu M. Security meter- a practical decision tree model to quantify risk. *IEEE Secur Priv* 2005, 3:18–24.
30. Sahinoglu M. An input-output measurable design for the security meter model to quantify and manage software security risk. *IEEE Trans Instrum Meas* 2008, 57:1251–1260.
31. Sahinoglu M. Can we quantitatively assess and manage risk of software privacy breaches? *IJCITAE* 2009, 3:65–70.
32. Sahinoglu M, Yuan YL, Banks D. Validation of a security and privacy risk metric using triple uniform product rule. *IJCITAE* 2010, 4:125–135.
33. Sahinoglu M. Generalized game theory applications to computer security risk. *Proceedings of the IEEE Symposium on Security and Privacy,* May 18–21, Oakland, CA.
34. Sohinoglu M. Security Meter-Quantitative Risk Assessment and Management with Game Theory Applications. Statistical and Applied Mathematical Sciences Institute (SAMSI) Symposium, *Proceedings of Interface/SAMSI Risk Conference,* May 22–24, 2008, Duke University, Durham, N. Carolina.
35. Benini M, Sicari S. Risk assessment in practice: a real case study. *Comput Commun* 2008, 31:3691–3699.
36. Fenz S, Ekelhart A. Verification, validation and evaluation in information security risk management. *IEEE Secur Priv* 2011, 9:58–65.
37. Banks D, Harris B. Adversarial risk analysis in counterterrorism. *57th Session of the International Statistical Institute (ISI09): Adversarial Risk Analysis - IPM 95* Aug 20, 2009, Durban, S. Africa.
38. Rios J, Rios D, Banks D. Adversarial risk analysis, influence diagrams, and auctions. *57th Session of the International Statistical Institute (ISI09): Adversarial Risk Analysis - IPM 95*, August 20, 2009, Durban, South Africa. Naval Research Logistics, 2011:1–13. doi:10.1002/nav.20469. wileyonlinelibrary.com.
39. Rios J, Rios D, Banks D. Adversarial Risk Analysis. *J Am Stat Assoc* 2009, 104:841–854. doi:10.1198/jasa.2009.0155. (Accessed 2011).
40. Singpurwalla ND. A framework for adversarial risk analysis. *57th Session of the International Statistical Institute (ISI09): Adversarial Risk Analysis - IPM 95,* Aug. 2009, Durban, South Africa.
41. Kiekintveld C, Jain M, Tsai J, Pita J, Ordóñez F, Tambe M. Computing optimal randomized resource allocations for massive security games. In: Decker, Sichman, Sierra Castelfranchi, eds. *Proceedings of 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2009)*; May 10–15, Budapest, Hungary; 2009, 689–696.
42. Herbert JP, Yao J. Game-theoretic risk analysis in decision-theoretic rough sets. *Proceedings of the 3rd International Conference on Rough Sets and Knowledge Technology*. Berlin, Heidelberg: Springer-Verlag; 2008.
43. He W, Xia C, Zhang C, Ji Y, Ma X. A network security risk assessment framework based on game theory. *Second International Conference on Future Generation Communication and Networking, FGCN'08*. Hainan Island, China, 2008, 249–253, 13–15.
44. He W, Xia C, Wang H, Zhang C, Ji Y. A game theoretical attack-defense model oriented to network security risk assessment. *International Conference on Computer Science and Software Engineering, FGCN'08*. Wuhan, China, 2008, 498–504, 12–14.
45. Shiva S, Simmons C, Ellis C, Dasgupta D, Wu Q. AVOIDIT: A cyber-attack taxonomy. Technical Report: CS-09-003, University of Memphis, August 2009.
46. Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q. A survey of game theory as applied to network security. *The 43rd Hawaii International Conference on System Sciences (HICSS), 5-8 January* 2010.
47. Shiva S, Roy S, Bedi H, Dasgupta D, Wu Q. A stochastic game with Imperfect Information for cyber security. *5th International Conference on i-Warfare & Security (ICIW)*, April 8–9, 2010, Ohio, USA.
48. Shiva S, Roy S, Ellis C, Datla V, Wu Q. On modeling & simulation of game theory-based defense mechanisms against DoS & DDoS attacks. *Proceedings of the 43rd Annual Simulation. Symposium (ANSS'10) in the Spring Simulation Multi-Conference* (*SpringSim*). Society for Modeling and Simulation International (SCS), Florida, USA.
49. Shiva S, Roy S, Dasgupta D. *Game theory for cyber security. In Sixth Cyber Security and Information Intelligence Research Workshop*. Oak Ridge, Tennessee, USA.: Oak Ridge National Laboratory; 2010.
50. Shiva S, Bedi H, Simmons C, Fisher M, Dharam R. Holistic game inspired defense architecture. *International Conference on Data Engineering and Internet Technology*. Bali Dynasty Resort, Bali, Indonesia, March, 2011.
51. Bedi H, Roy S, Shiva S. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, part of (SSCI) April 2011, Paris, France.
52. Manshai MH, Zhu, Q, Alpcan T, Basar T, Hubaux J. Game theory meets network security and privacy. *ACM Trans Comput Logic* 2010, 5:1–35.

53. Luo Y, Szidarovzky F, Nashif Y, Hariri S. Game theory based network security. *J Inf Secur* 2010, 1:41–44. Available at: http://www.SciRP.org/journal/jis (pub. online July 2010)
54. Wang S, Banks D. Network Routing for Insurgency: An Adversarial Risk Analysis Framework. *Nav Res Logist* 2011, 58:595–607.
55. Anderson DR, Sweeney DJ, Williams TA. Martin K. *An Introduction to Management Science—Quantitative Approaches to Decision Making*. 12th ed. Mason: OH: Thompson/South-Western; 2008, 241–252.
56. Colman AM. *Game Theory & Its Applications*. Oxford: Butterworth-Heinemann Ltd.; 1982, 1995.
57. Singh A, Lakhotia A. Strategic methods in adversarial classifier combination. *CRW'10: 3rd Cyberspace Research Workshop*, Nov. 15, 2010; Shreveport, LA, USA. Available at: http://csc.latech.edu/crw10/. (Accessed 2011).
58. Maille P, Reichl P, Tuffin B. Of threats and costs: a game -theoretic approach to security risk management. In: Gulpinar N. et al., eds. *Performance Models and Risk Management in Communications Systems, Springer Optimization and Its Application*. Springer Science + Business Media, LLC 2011, 46, doi:10.1007/978-14419-0534-5_2.
59. Papadopoulou V, Gregoriades A. Nonfunctional requirements validation using Nash equilibria. In: Mamun Habib, ed. *Management and Services (Open Access Book)*, ISBN 978-953-307-118-3. InTech; October 2010, 112.
60. Rothkopf M. Decision analysis: the right tool for auctions. *Decis Anal* 2007, 4:167–172.
61. Sahinoglu M. *Trustworthy Computing: Analytical and Quantitative Engineering Evaluation (CD ROM included)*. New York: John Wiley & Sons Inc.; 2007.
62. Sahinoglu, M. National cyber-security risk assessment and management. *AFITC (Air Force Information Technology Conference)* August 2010, Montgomery, AL. USA.
63. Eisenhower Series Invited Speaker, Air War College, Maxwell AFB, Montgomery AL, April 2011. Available at: www.aum.edu/csis. (Accessed 2011).
64. Sahinoglu, M. Some interdisciplinary topics on game-theoretical solutions for quantitative cyber-risk estimation and management. *Computing Science and Statistics, Proceedings of the 42nd Symposium on the Interface*. Cary, NC: SAS Institute; June 1–3, 2011.
65. Sahinoglu, M. Quantitative Risk Assessment of Software Security and Privacy, and Risk Management with Game Theory. Invited Speaker, *CERIAS/Purdue University Annual Symposium Seminar*, W. Lafayette, IN; Feb 11, 2009.
66. Sahinoglu M. World ecological risk assessment and management. *AFITC (Air Force Information Technology Conference)*. August 2009, Montgomery, AL, USA.
67. Akkaya AD, Sahinoglu M, Morton S. Phoha V. A quantitative security and privacy risk assessment and management method for social networks. *IPS018 (Invited Session on Trustworthy Computing), ISI 2011* Dublin, Ireland, August 22–26, 2011. Available at: http://127.0.0.1:9000/\penalty\@Mshowabstract.php?congress=ISI2011&id=121. (Accessed 2011).
68. Sahinoglu M. Method for cyber-security risk assessment and cost-efficient management in wireless sensor networks. *CRW'10: 3rd Cyberspace Research Workshop*, Nov. 15, 2010, Shreveport, LA, USA. Available at: http://csc.latech.edu/crw10/. (Accessed 2011).
69. Sahinoglu M. Cybersystems and information security: Master of Science program at Auburn University Montgomery. *GSTF Int J Comput* 2011, 1:71–76.