Game Theory and Cyber Defense

Abderrahmane Sokri

Abstract The extensive use of information technology systems in military sector has changed the face of the battlefield and the nature of war. A growing body of literature argues that the game-theoretic reasoning is well-suited to many problems in cyber defense. A game between a defender and an attacker trying to gain access to computers remotely is a typical strategic interaction in this domain. This chapter discusses how game theory can be applied in cyberspace. It offers a comprehensive review of literature on the application of game theory in this area. It proposes and illustrates a new game formulation combining game theory and other techniques. The chapter highlights the recognized challenges associated with the applicability of game theory in the cyber world. It discusses how the game-theoretic formalism can be adapted to obtain sound solutions in a reasonable time.

Keywords Game theory · Cyber defense · Cyberattack · Cybersecurity · Common knowledge

> [The] cyber threat is one of the most serious economic and national security challenges we face as a nation. —President Barack Obama, 29 May 2009

1 Introduction

Revolutionary advancement in information and communication technologies (ICT) has brought many changes to the nature of war. Cyberspace has become both a crucial enabler and a critical vulnerability for military forces. It has become the new battlefield, on par with air, land, and maritime, but with its own lot of complex and

A. Sokri (✉)
Government of Canada, Department of National Defence, Ottawa, ON, Canada
e-mail: Abderrahmane.Sokri@drdc-rddc.gc.ca

P.-O. Pineau et al. (eds.), *Games in Management Science*,
International Series in Operations Research & Management Science 280,
https://doi.org/10.1007/978-3-030-19107-8_18

challenging problems. The cyber weapons could be social engineering, upgraded viruses, Trojan horses, worms, flooding denial-of-service (DoS), distributed denial-of-service (DDoS) or botnets, and advanced persistent threat (APTs) (Bernier et al. 2012; Aslanoglu and Tekir 2012).

In a social engineering attack, an attacker pieces together enough information to infiltrate an organization's network. The attacker can, for example, claim to be a new employee, repair person, or researcher and ask questions to different sources about an organization or its computer systems. A virus is a computer program designed to deliberately damage files or spread to other computers. A Trojan horse is a computer program with a good purpose that hides a damaging program that performs a malicious action. A worm is a virus that can spread from a computer to another without human interaction. It takes up memory, exhausts network bandwidth, and causes a computer to stop responding. It can also allow attackers to gain access to computers remotely. Most of these threats are included as attachments or links contained in email messages.

A DoS attack occurs when an attacker prevents legitimate users from accessing information or services such as email and online banking accounts. In this attack, an attacker overloads a network or server with information or requests. In a DDoS attack, an attacker takes advantage of security weaknesses to control multiple computers. These computers are used afterward to launch a DoS attack (McDowell 2009). These attacks can cause public or private institutions to lose important data, money, or their reputations (Liang and Xiao 2013). APTs use sophisticated techniques to monitor and extract sensitive data from a specific target over a long period of time while remaining undetected.

These cyber weapons are shaped based on the knowledge of target's vulnerabilities. The National Institute of Standards and Technology (NIST) defines vulnerability as a weakness in system security procedures, design, internal controls, or implementation that could be exploited by a threat source (NIST 2002). A vulnerability is exploitable when an attacker has the knowledge about it and the skills to exploit it.

Vulnerabilities are characterized by their dynamic nature. When a vulnerability is detected by the defender, the attacker's weapon exploiting it becomes useless and the target's defense becomes upgraded. This refers to the two paradoxes of cyber weapons. The first paradox states that cyber weapons are subject to time decay. The second paradox states that cyber weapons usage may shortly enhance the target's defense (Podins and Czosseck 2012).

Without being directly lethal, cyberattacks can cause loss of data confidentiality (e.g., unauthorized disclosure of information), integrity (e.g., unauthorized modification of information), or availability (e.g., disruption of access) (Bowen et al. 2006). It can also cause damage or destruction of equipment (Ziolkowski 2010; Podins and Czosseck 2012). The extent and severity of cyberattacks vary from local (loss of email confidentiality) to nation-wide (Ottis 2008). But without exploitable vulnerabilities, cyberattacks would be limited to DoS, DDOS, and social engineering attacks (Moore et al. 2010; Podins and Czosseck 2012).

In 2007, Estonia was the subject of the first massive nation-wide cyberattack in the world. A campaign of cyberattacks was conducted during 3 weeks against government websites, banks, critical national infrastructure, newspapers, and broadcasters. Attacks included massive DDoS, phishing, email spam, and website defacing (Aslanoglu and Tekir 2012; van Vuuren et al. 2012; Podins and Czosseck 2012).

In 2009, an APT exploited a previously unknown vulnerability in Internet Explorer to compromise systems at Google, Adobe, and more than 30 large companies. The main objective was to steal intellectual property from these security and defense contractor companies (Aslanoglu and Tekir 2012).

In 2010, the Stuxnet worm against the Iranian nuclear program was considered as the real start of cyber warfare (Adams et al. 2012). This unprecedented and highly sophisticated attack infected more than 30,000 computers in Iran. The virus continued to spread via Internet and infect about the same number of computers in other countries including the USA, the UK, China, and Germany.

This attack has changed the face of the battlefield and has broken down a common belief stating that control systems are protected, if (1) nothing on computers connects to the Internet, (2) new memory sticks are used for data exchange, and (3) viruses are detectable by the unusual behavior of computers (Miyachi et al. 2011; Aslanoglu and Tekir 2012; Podins and Czosseck 2012).

In 2013, Target Corporation came under an APT resulting in an unauthorized access to credit card numbers and personal information of 40 million customers (Acquaviva 2017). Since then, there has been a growing discussion about the best ways to protect potential target areas against offensive cyberattacks (Bier et al. 2009). To overcome these problems, a variety of protective and reactive measures have been employed. As shown in Table 1, traditional network security techniques include (1) tamperproof techniques, (2) cryptography, (3) detection and prevention techniques, (4) honeypots, and (5) technical attribution.

Although these techniques are crucial mechanisms for cybersecurity, they are not a panacea (Roy et al. 2010). They may be sufficient against casual attackers using well-known techniques, but the complex cybersecurity problem is still far from being completely solved. There is a continuous race between attackers and security specialists. When a smart security solution is proposed a smarter way to circumvent, it is found. There will be an ongoing and challenging need to design tools that protect our systems and networks against sophisticated and well-organized adversaries (Roy et al. 2010).

Many researchers including Roy et al. (2010), Zakrzewska and Ferragut (2011), Kiekintveld et al. (2015), and Tambe (2011) have argued that the game-theoretic reasoning is well-suited to many problems in network security and cyber warfare. This mathematical approach examines how agents or players might act when trying to optimize a utility function (Acquaviva 2017). The United States Department of Defense (DoD), for example, states that applying game theory techniques in cyberspace may assist in analyzing an adversary's preferred tactics (DoD 2011). Game theory can also guide resource allocations to defend against intelligent antagonists by explicitly taking into account the intelligent and adaptive nature of

Table 1 Traditional protective and reactive measures in cyberspace

Technique	Definition
Tamperproof	Automated methods of identification based on unique measurable physiological or behavioral characteristics such as voice, fingerprints, or iris patterns (Matyas and Riha 2002)
Cryptography	Techniques that merge words with images to hide data in transit or storage. They are used for authentication of user and data.
Detection/prevention	Techniques including antivirus software, firewalls, and intrusion detection systems (IDS) Antivirus programs scan the communication mediums and the storage devices, detect signs of malware presence, and remove them. Firewalls limit access to private networks connected to the Internet. IDS algorithms detect suspected intrusions and alert the network administrator in real time (Gueye 2011; Roy et al. 2010)
Honeypot	A fake computer system used in network security to waste the attacker's time and resources. The network administrator can also use the captured data from the attacker's actions to better protect the network. (McCarty 2003; Rowe et al. 2007; Carroll and Grosu 2011; Pibil et al. 2012)
Attribution	Attribution is the determination of the identity or the location of an attacker or an attacker's intermediary (Robinson et al. 2015; Wheeler and Larsen 2003). The identity can be physical such as a geographical address or digital such as an Internet Protocol (IP) address (Guan and Zhang 2010). The information captured by attribution can be used to improve defensive techniques and prevent future attacks (Nicholson et al. 2012)

the threat (Bier et al. 2009). The arguments put forward to justify this approach are numerous. They particularly include (but are not limited to) its ability to model the non-cooperative and cooperative strategic interactions between multiple decision-makers with conflicting goals. The analytical setting may be static or dynamic, discrete or continuous, deterministic or stochastic, and linear or non-linear.

A cooperative game model examines how players might be working together to optimize a collective utility function (Acquaviva 2017). Cooperative games describe at high level the structure, strategies, and payoffs of subsets of players or coalitions. They are generally characterized by a characteristic function describing the outcome of each coalition.

A typical cooperative game in cyber domain may include a number of organizations or countries exchanging vulnerability information and attack detection procedures. By exchanging information on vulnerabilities, each member of the coalition will build new weapons using the newly learned vulnerabilities (Podins and Czosseck 2012). The UK government, for example, has initiated a cybersecurity hub that enables the exchange of information on cybersecurity threats between the public and private sectors (van Vuuren et al. 2012).

In a non-cooperative game, players seek to optimize their individual utility functions regardless of the utilities of the other players involved (Acquaviva 2017). Non-cooperative games are more general than cooperative games. They describe in

detail the individual strategies and payoffs of each player. They focus on analyzing Nash equilibrium that no player can do better by unilaterally deviating from it (Breton et al. 2008; Bachrach et al. 2013; Brandenburger 2007).

Interactions in cyberspace are generally adversarial and inherently selfish. A game between a system administrator and an attacker trying to compromise or destroy the system is a typical non-cooperative game in this domain. In this case, the time spent controlling the system or the reward for destroying it may be the utility function for the attacker. The reward for controlling the system may be the utility function for the defender (Acquaviva 2017).

The aim of this chapter is to discuss the suitability of game theory to adversarial interaction between attackers and defenders in cyberspace. The chapter also sheds light on the main challenging issues surrounding its applicability in this domain. A new game formulation combining simulation and game-theoretic approaches is proposed to solve the problem of uncertain observability in the payoff matrix.

This chapter is organized into six sections. Following the introduction, Sect. 2 provides a comprehensive review of literature on the application of game theory in the cyber domain. Section 3 presents a resource allocation problem to show how the new approach can be used in cyberspace. In Sect. 4, a case study is presented to illustrate the suggested approach. The main challenges associated with the applicability of game-theoretic methods in cyberspace are discussed in Sect. 5. Concluding remarks as well as future research directions are indicated in Sect. 6.

2 Literature Review

Game theory is a common formalized way to inspire the development of defense algorithms in the physical world (Moisan and Gonzalez 2017; Coniglio 2013; Tambe 2011; Roy et al. 2010). A growing body of literature recognizes game theory as a sound theoretical foundation for modeling the strategic interactions between selfish agents in the cyber world. This literature can be divided into three main categories: resource allocation, network security, and cooperation models.

2.1 Resource Allocation

Game theory can guide resource allocations to defend against intelligent attacks by explicitly taking into account the adaptive nature of the threat. In this game, the defender seeks to find the optimal resource allocation that maximizes his payoffs. The attacker seeks to minimize the risk of being traced back and punished (Acquaviva 2017). This problem is known in the game-theoretic literature as the allocation game (Bier et al. 2009).

Fielder et al. (2014), for example, proposed a game-theoretic model to optimally allocate cybersecurity resources such as administrators' time across different tasks.

In this game, the defender's solution is optimal independently from the attacker's strategy. The authors also found that a particular Nash equilibrium provides the most effective defense strategy and used real-life statistics to validate their result. More recently, Sokri (2018) used an allocation game to analyze the problem of common knowledge in cyberspace. The author incorporated uncertainty on each imprecise variable by changing its static value to a range of values.

Game theory is also used to determine the optimal investment in critical infrastructures such as networked systems. In this case, defensive investment is used to increase the effort needed by an attacker to achieve a certain probability of success. It can also be used to reduce the success probability of an attack, rather than increasing its effort. The game-theoretic framework determines the optimal allocation of the total defensive budget over the various components of the system in order to minimize the success probability of a potential attack or to maximize its expected cost (Azaiez and Bier 2007).

Game theory can also be used to investigate the optimal strategies for managing a sensitive security resource in response to APTs. Depending on the setting being modeled, the resource may be a password or an entire infrastructure. FlipIt, for example, is a two-player dynamic game where players may take control of the resource at any time by executing a stealthy move (i.e., not immediately detected). This idea implies that each player is allowed to move at arbitrary points in time, and the timing of the moves may be kept hidden from the other player. The objective is to maximize the fraction of time the player controls the resource while minimizing the cumulative move cost. FlipIt is characterized by the idea of stealthy moves or stealthy takeover (Rasouli et al. 2014; Hobbs 2015).

2.2 Network Security

Game theory has also been proposed by several studies to understand defense strategies in network security. It offers a sound theoretical foundation for managing information security, modeling the strategic interactions in intrusion detection, and analyzing network defense mechanism design. It is useful for generalization of problems, formalizing the existing ad-hoc schemes, and future research (Alpcan and Basar 2004).

Bloem et al. (2006), for example, developed a stochastic and dynamic game to examine intrusion detection in access control systems. The authors used a game-theoretic approach to model the interaction between an attacker and a distributed IDS. They introduced the sensor network as a third player with a fixed probability distribution representing the output of the sensor network during the attack. The authors discussed the properties of the resulting system analytically and numerically.

Roy et al. (2010) presented a taxonomy for classifying the existing game-theoretic solutions designed to enhance network security. The authors provided a systematic description of how games can be played and what the outcomes might

be. This information is used to define games with relevant concepts for network security problems.

Jafarian et al. (2013) combined game theory and constraint satisfaction optimization to proactively defend against denial-of-service attacks. In this static game, Nash equilibrium is determined by players' strategies and the cost associated with them. The optimal strategy for attack deterrence is determined while satisfying security and performance requirements of the network. Results showed that the method improves the protection of flow packets from being attacked against persistent attackers without causing any disruption for flows.

More recently, Musman and Turner (2018) described a game-oriented approach to minimizing cybersecurity risks for a given investment level. The game formulation uses the defender strategies to minimize the maximum cyber risk. The interested reader is referred to Information Resources Management Association (2018) for further information on this topic.

Game theory has also been used for studying the effects of deception on the interactions between an attacker and a defender of a computer network (Baston and Bostock 1988). In this literature, the defender can employ camouflage by disguising, for example, a honeypot as a normal system. Deception increases the attackers' uncertainty and effort (e.g., time and money) to determine whether a system is true or fake. Even long before computers existed, deception was widely used for information protection (Cohen 1998; Rowe et al. 2007; Carroll and Grosu 2011). Rowe et al. (2007), for example, summarized some game-theoretic aspects of introducing honeypots. The authors developed a mathematical model of deception and counterdeception to see at what point people could detect deception. Results show that attacks on honeypots decreased over time.

Carroll and Grosu (2011) performed a game-theoretical investigation of deception in network security. The authors used a dynamic game of incomplete information to examine a scenario where a defender can disguise normal systems as honeypots or honeypots as normal systems. The attacker observes the system and decides whether or not to proceed compromising the system. The authors determined and characterized the perfect Bayesian equilibria of the game. At an equilibrium, the players do not have any incentives to unilaterally deviate by changing their strategies.

2.3 Agent Cooperation

Cooperative game theory can determine how the collective reward can be shared between selfish agents. It can also provide a mechanism to sustain the cooperative solution which is not a self-enforcing contract (Breton et al. 2008). A typical cooperative game in the existing literature may include a number of selfish agents and a principal controlling a computer network. To allow a reliable connectivity between a certain set of critical servers, the principal can incentivize the agents to cooperate by offering them a certain reward (Bachrach et al. 2013). It can also

consist of a multi-mode attack combining different types of warfare that are more effective in tandem than when employed alone (Browne 2000).

Liu et al. (2005), for example, developed a preliminary game-theoretic formalization to capture the interdependency between attacker and defender objectives and strategies. The authors showed that the concept of incentives and utilities can be used to model attacker objectives. Bachrach et al. (2013) modeled a communication network where a failure of one node may disturb communication between other nodes as a simple coalitional game. The authors showed how various game-theoretic solution concepts can be used to characterize the fair share of the revenues an agent is entitled to.

Shamshirband et al. (2014) combined a game-theoretic approach and a fuzzy Q-learning algorithm in Wireless Sensor Networks. The authors implemented cooperative defense counter-attack scenarios for the victim node and the base station to operate as rational decision-maker players through a game theory strategy. The proposed model's attack detection and defense accuracy yield a greater improvement than the existing machine learning methods.

A recent survey of the existing game-theoretic approaches for cybersecurity can be found in Do et al. (2017).

3 Resource Allocation Game

In this section, we will show how a game-theoretic model can be used to optimally allocate resources in the cyber domain. The main challenges and open research questions associated with this formulation will be presented and discussed in Sect. 5.

Consider a security game between an attacker a and a defender d in a cyberinfrastructure system. Following Korzhyk et al. (2011), let $A = \{t_1, t_2, \ \ldots \ , t_n\}$ be a set of n targets that the attacker may choose to attack. The defender seeks to prevent attacks by covering targets using cybersecurity resources from the set $R = \{r_1, r_2, \ \ldots \ , r_m\}$. In the physical world, targets may be flights and resources may be air marshals. In the cyber world, targets may be software vulnerabilities and resources may be protective devices such as firewalls (Gueye 2011).

The set A corresponds to pure strategies for the attacker where each pure strategy refers to a single target to attack. Let D be the set of all the possible resource allocations over the set of targets. If at most one resource is assigned to a target, there will be n *Choose* m combinations to allocate m resources to n targets (Jain et al. 2010). The defender pure strategies are represented by these resource allocations. The two players are allowed to play mixed strategies by assigning a probability distribution over the set of pure strategies (Coniglio 2013; Jain et al. 2010). If a player adopts his mixed strategy, the outcome of the game will be expressed as an expected value.

Let δ be a leader's mixed strategy consisting of a vector of the defender's pure strategies. Denote by δ_i the proportion of times assigned to the pure strategy i when the defender plays the mixed strategy δ.

Similarly, we denote by ρ a mixed strategy of the attacker (the follower) and by ρ_j the probability of the pure strategy j when he plays the mixed strategy ρ. Let $E(U_d(i,j))$ be the expected utility of the defender and $E(U_a(i,j))$ the expected utility of the attacker when the defender plays pure strategy i and the attacker plays pure strategy j.

One of the main challenging issues in security games is the problem of common knowledge concept. It is generally assumed in these games that the players are able to exactly evaluate their own payoffs and the payoffs of their opponents. In most real-world cybersecurity problems, this assumption is not always true. Using deterministic values of payoffs may make the committed strategies ineffective (Coniglio 2013; Sokri 2018). In this paper, utilities are seen as random variables generated by a stochastic simulation. Uncertainty is incorporated in the theoretical framework using their expected values.

Fixing the policy of the defender to some mixed strategy δ, the first problem to solve is to find the attacker's best response to δ. This optimization problem can be formulated as a linear program where the follower maximizes his expected utility given δ.

$$\text{Max}_{\rho} \sum\nolimits_{i \in D} \sum\nolimits_{j \in A} \delta_i \rho_j E\left(U_a\left(i, j\right)\right) \tag{1}$$

$$\text{s.t.} \sum\nolimits_{j \in A} \rho_j = 1 \tag{2}$$

$$\rho_j \geq 0, \forall j. \tag{3}$$

While the constraints define the set of feasible solutions ρ as a probability distribution over the set of targets A, it is straightforward to see that the optimal strategy for the follower is a pure strategy $\rho_j = 1$ for a j that maximizes $\sum_{j \in A} \delta_i E\left(U_a\left(i, j\right)\right)$. This result can also be obtained using the corresponding dual problem which has the same optimal solution value

$$\text{Min}_{v}\ v \tag{4}$$

$$\text{s.t.} v \geq \sum\nolimits_{i \in D} \delta_i E\left(U_a\left(i, j\right)\right), \quad j \in A. \tag{5}$$

The corresponding complementary slackness condition is given by

$$\rho_j \left(v - \sum\nolimits_{i \in D} \delta_i E\left(U_a\left(i, j\right)\right)\right) = 0, \quad j \in A. \tag{6}$$

This condition implies that the follower expected reward is maximal for any pure strategy with $\rho_j > 0$.

Denoting by $\rho(\delta)$ the follower's best response to δ, the leader seeks to solve the following problem:

$$\text{Max}_{\rho} \sum_{i \in D} \sum_{j \in A} \delta_i \rho(\delta)_j E\left(U_d\left(i, j\right)\right) \tag{7}$$

$$\text{s.t.} \sum_{i \in D} \delta_i = 1 \tag{8}$$

$$\delta_i \in [0, 1], \quad \forall i \in D. \tag{9}$$

The two constraints enforce the leader's mixed strategy to be feasible.

If we complete the leader's problem by including the follower's optimality conditions, the two programs can be formulated as a single mixed-integer quadratic problem (MIQP).

$$\text{Max}_{\delta, \rho, v} \sum_{i \in D} \sum_{j \in A} \delta_i \rho_j E\left(U_d\left(i, j\right)\right) \tag{10}$$

$$\text{s.t.} \sum_{i \in D} \delta_i = 1 \tag{11}$$

$$\sum_{j \in A} \rho_j = 1 \tag{12}$$

$$0 \leq \left(v - \sum_{i \in D} \delta_i U_a\left(i, j\right)\right) \leq \left(1 - \rho_j\right) M, \quad \forall j \in A \tag{13}$$

$$\delta_i \in [0, 1], \quad \forall i \in D \tag{14}$$

$$\rho_j \in \{0, 1\}, \quad \forall j \in A \tag{15}$$

$$v \in R \tag{16}$$

To simplify the complementary slackness condition represented by the rightmost inequality in Eq. (13), the attacker plays only pure strategies. Equations (12) and (15) characterize a feasible pure strategy for this player. In this formulation, v is the follower's maximum payoff value and M is a large number.

4 Illustration

To illustrate the approach suggested in Sect. 3, consider the game in compact form in Table 2 (Sokri 2018; Jain et al. 2010; An et al. 2011). In this example, there are three targets and two defender resources. Each of defender's resources can only cover one target at a time. For each target, there are two payoffs: the payoff of the attacker and the payoff of the defender. Each payoff consists of two parts: one when the attacked target is covered and one when it's uncovered.

Let $U_d^c(t)$ be the defender's payoff if the attacked target t is covered and $U_d^u(t)$ his payoff if the target is uncovered. Similarly, denote by $U_a^u(t)$ the attacker's payoff if the attacked target t is uncovered and by $U_a^c(t)$ the attacker's payoff if the attacked target t is covered. For each target t, the expected utilities of the defender and the attacker are respectively given by

$$U_d(t) = \rho_t \left(\delta_t U_d^c(t) + (1 - \delta_t)\, U_d^u(t)\right) \tag{17}$$

$$U_a(t) = \rho_t \left((1 - \delta_t)\, U_a^u(t) + \delta_t U_a^c(t)\right) \tag{18}$$

The expected utilities in Eqs. (17) and (18) depend simply on the attacked targets and their coverage. Uncertainty can furthermore be placed on each payoff using three-point estimates instead of single values.

This game has multiple equilibria of the form

$$\langle \delta = (\delta_1, \delta_2, 1)\,, \quad \rho = (0, 0, 1) \rangle\,. \tag{19}$$

This standard solution indicates that the attacker would aim the most valuable target no matter how defended it might be (Sokri 2018; Jain et al. 2010; An et al. 2011). A solution for the defender–attacker Stackelberg game that satisfies the constraints and the numerical convergence criterion is given by

$$\langle \delta = (0.75, 0.25, 1)\,, \quad \rho = (0, 0, 1) \rangle\,. \tag{20}$$

To find a robust solution, further refinement is needed. The equilibrium refinement may be based on some utility dominance criteria such as Pareto dominance (An et al. 2011).

Table 2 Payoff table

	Defender		Attacker	
	Covered	uncovered	uncovered	Covered
Target 1	5	2	7	5
Target 2	2	1	4	4
Target 3	5	5	12	9

5 Application of the Game in Cyberspace: Challenges and Opportunities

Game theory has already produced several notable successes in numerous physical security domains. It was applied, for example, to randomize checkpoints at the Los Angeles International Airport (LAX), to assign federal air marshals to protect flights (Jain et al. 2010; Kiekintveld et al. 2015; Acquaviva 2017). Researchers have also used game theory to understand security and defense strategies in the cyber world. The application of game theory to this domain presents at least three main challenges: (1) the complexity of the cyber domain, (2) the dynamic nature of the analyzed games, and (3) the validity of the adopted assumptions.

5.1 Complexity of the Cyber Domain

Cybersecurity is more complex than in physical security domains. In the cyber domain, digital attacks are often sophisticated and imperceptible to the human senses. They are highly dynamic overstepping all geographic and political boundaries (Moisan and Gonzalez 2017). To interact appropriately in the cyber domain under dynamically changing real-world scenarios, it is important to understand the entire cyberinfrastructure system. To this end, the holistic game inspired defense architecture suggested by Shiva et al. (2012) would be a good starting point.

Shiva et al. (2012) proposed a four-layer decision-making framework inspired by game theory. As illustrated in Fig. 1, the security scheme is organized into four layers. The first and innermost layer in the framework contains self-checking hardware and software components. The second layer consists of secure built-in or bolt-on applications employing self-checking concepts and components. The

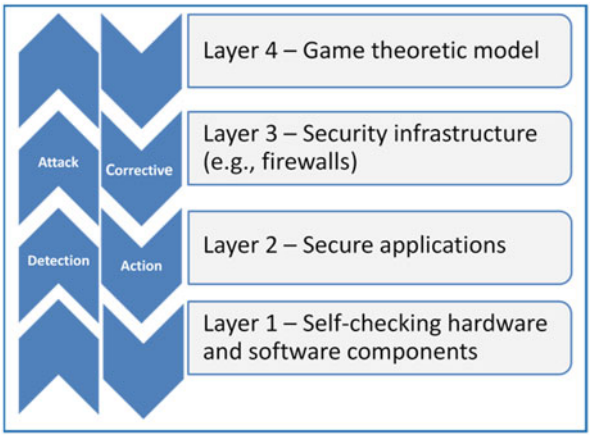

Fig. 1 Game inspired decision model (Adapted from Shiva et al. 2012)

third layer is the security infrastructure consisting of intrusion detection system (IDS), firewalls, and antivirus software. The fourth and outermost layer uses game-theoretic analysis to provide the best action strategies. It receives input from the inner three layers, evaluates the committed or probable attack information, and elects the optimal decision for defense.

5.2 Static Versus Dynamic Perspectives

A static model is a model where the system state is independent of time. It is an interaction where each player makes a single decision in isolation and under imperfect information. The well-known prisoner's dilemma falls under the category of static games. Decisions in static games can be seen as made simultaneously. Real-world security interactions are inherently dynamic where recent attacks are built upon previous attacks. A dynamic model is a model where the system state changes with time, and players are able to observe the outcome of previous moves before responding. Stealthy move games are examples of dynamic games. The dynamic perspective can be introduced to the suggested framework by playing the game within a finite or infinite time horizon. Factors that determine the objective function such as rewards and costs should be explicitly presented as functions of time. This addition can, however, result in a more complex and challenging problem.

5.3 Validity of Assumptions

The game-theoretic framework in Sect. 3 relies on two main key assumptions. The game considers (1) two rational players with certain observability and (2) limited amount of homogeneous resources and targets with no explicit cost of moving. In real world, the defender may face multiple rational or irrational attackers, and the common knowledge on payoffs may be missing. The number of targets to be protected can be large and the attacker may aim more than a single target. The defender's resources may also be numerous and with explicit cost of moving. By making the formalism more realistic, the algorithm would not be able to find an optimal solution in a reasonable time. It is, therefore, necessary to combine game theory with other potential tools and techniques to enhance cyber conflict analysis. Table 3, adapted from DoD (2011), presents the potential techniques, their definitions, and their potential use in cyberspace.

Combining game theory with other techniques in cyberspace is still at its beginnings, and many open issues are still to be tackled. The future combined frameworks should be able:

Table 3 Potential tools and techniques that may be combined in cyber conflict analysis

Technique	Definition	Use in cyberspace
Game theory	The study of mathematical models of conflict and cooperation between intelligent rational decision-makers (Myerson 1991)	Investigate security decisions in a methodical manner
Computer simulation	Computer representations that model the real-world interactions	Process visualization Variables and parameters randomization War gaming
Genetic algorithms	A family of computational models inspired by evolution	Searching for a sequence of steps that will allow an adversary to achieve their objective
Graph theory	A graph is a set of nodes and links that models pairwise relationships between items	Network mapping Bayesian network Identification of strong and weak links and nodes in the adversary's critical requirements
Reliability modeling	The process of predicting the likelihood that a component or system will function prior to its implementation	Analyze the availability of a critical capability when resources and conditions are deficient or absent
Cyber forensic analysis	Methods to recover and analyze materials found in digital sources	Reconstructing events believed to be malicious
IDS	A device or software application that monitors a computer network or individual system for abnormal activity	Detect the step executed and initiate mitigation measures

- To be dynamic where recent attacks are built upon previous ones;
- To model multiple self-interested agents (e.g., multiple unknown attackers from multiple locations);
- To handle multiple uncertainties in adversary payoffs and observations;
- To deal with bounded rationality of human adversaries by introducing stochastic actions.

6 Conclusion

The extensive use of ICT in military sector has changed the face of the battlefield and made cybersecurity an increasingly important concern. Cyber weapons are malicious software that exploit unknown vulnerabilities in the target's defense. The players in this new space can be individuals, devices, or software. Theirs interactions are generally non-cooperative and their objectives are inherently conflicting.

The game-theoretic reasoning has been recognized as well-suited to many problems in the cyber world.

The arguments put forward to justify its use are abundant. Game theory uses proven mathematics to investigate a large range of security decisions. It provides a sound theoretical foundation for understanding the strategic interactions between selfish agents and optimally allocating limited resources and sharing collective rewards.

Defense algorithms inspired by game theory have become very popular in the physical security world. Cyberinfrastructure systems are, however, more complex and the corresponding security threats are highly dynamic and sophisticated. Despite considerable effort from the research community, the application of game theory in cyber defense is still at its beginnings and needs further adaptation to deliver according to its potential.

Current cyber algorithms generally use static settings and rely on idealized assumptions such as common knowledge about the payoff matrix. They also assume that players are able to remember and process large amounts of information accurately. Applying game theory under these simplified conditions may make the resulting strategies ineffective. Scaling up the formalism to real-world-sized problems would make it very complex and intractable.

To be able to make the formalism more realistic and obtain sound and effective solutions in a reasonable time, we recommend combining game theory with other techniques and tools. The suggested techniques include computer simulation, genetic algorithms, graph theory, reliability modeling, and cyber forensic analysis. Tools may consist of IDS, firewalls, and antivirus software. Using these techniques and tools under a solid game-theoretic setting will provide huge potential to solve many cybersecurity standard problems.

References

Acquaviva, J. R. (2017). *Optimal cyber-defence strategies for advanced persistent threats: A game theoretical analysis*. Master Thesis, The Pennsylvania State University.

Adams, A., Reich, P., & Weinstein, S. (2012). A non-militarised approach to cyber-security. In E. Filiol & R. Erra (Eds.), *Proceedings of the 11th European Conference on Information Warfare and Security* (pp. 1–8). Laval: Academic Conferences & Publishing International Ltd.

Alpcan, T., & Basar, T. A. (2004). Game theoretic approach to decision and analysis in network intrusion detection. In *Proceedings of the 42nd IEEE Conference on Decision and Control*. Hawaii: IEEE.

An, B., Tambe, M., Ordonez, F., Shieh, E., & Kiekintveld, C. (2011). Refinement of strong Stackelberg equilibria in security games. In *Proceedings of the 25th Conference on Artificial Intelligence* (pp. 587–593). Los Alamitos, CA: IEEE.

Aslanoglu, R., & Tekir, S. (2012). Recent cyberwar spectrum and its analysis. In *Proceedings of the 11th European Conference on Information Warfare and Security* (pp. 45–52). Laval: Academic Conferences & Publishing International Ltd..

Azaiez, N., & Bier, V. M. (2007). Optimal resource allocation for security in reliability systems. *European Journal of Operational Research, 181*(2), 773–786.

Bachrach, Y., Porat, E., & Rosenschein, J. S. (2013). Sharing rewards in cooperative connectivity games. *Journal of Artificial Intelligence Research, 47*, 281–311.

Baston, V. J., & Bostock, F. A. (1988). Deception games. *International Journal of Game Theory, 17*(2), 129–134.

Bernier, M., LeBlanc, S., & Morton, B. (2012). Metrics framework of cyber operations on command and control. In *Proceedings of the 11th European Conference on Information Warfare and Security* (pp. 53–62). Laval: Academic Conferences & Publishing International Ltd..

Bier, V. M., Cox, L. A., & Azaiez, M. N. (2009). Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks (chapter 1). In V. M. Bier & M. N. Azaiez (Eds.), *Game theoretic risk analysis of security threats* (pp. 1–11). New York: Springer.

Bloem, M., Alpcan, T., & Basar, T. (2006). Intrusion response as a resource allocation problem. In *IEEE Conference on Decision and Control*. Piscataway, NJ: IEEE.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers*. Gaithersburg, MD: NIST Special Publication 800–100.

Brandenburger, A. (2007). *Cooperative game theory: Characteristic functions, allocations, marginal contribution*. New York: Stern School of Business, New York University.

Breton, M., Sokri, A., & Zaccour, G. (2008). Incentive equilibrium in an overlapping-generations environmental game. *European Journal of Operational Research, 185*(2), 687–699.

Browne, R. (2000). C4I defensive infrastructure for survivability against multi-mode attacks. In *Proceedings of 21st Century Military Communication-Architectures and Technologies for Information Superiority*. Piscataway, NJ: IEEE.

Carroll, T. E., & Grosu, D. (2011). A game theoretic investigation of deception in network security. *Security and Communication Networks, 4*(10), 1162–1172.

Cohen, F. (1998). A note on the role of deception in information protection. *Computers and Security, 17*(6), 483–506.

Coniglio, S. (2013). *Algorithms for finding leader-follower equilibrium with multiple followers*. Ph.D. Thesis, Politecnico di Milano.

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N., & Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR), 50*(2), 30.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Game theory meets information security management. In *Information Security and Privacy Conference* (pp. 15–29). Berlin: Springer.

Guan, Y., & Zhang, L. (2010). Network forensics. In J. R. Vacca (Ed.), *Managing information security* (pp. 197–212). Rockland, MA: Syngress.

Gueye, A. (2011). *A game theoretical approach to communication security*. Ph.D. Dissertation, University of California.

Hobbs, J. (2015). *Dominion: A game of information exploitation*. Master Thesis, University of New Mexico.

Information Resources Management Association. (2018). *Game theory: Breakthroughs in research and practice* (1st ed.). Hershey PA: IGI Global.

Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2013). Formal approach for route agility against persistent attackers. In *18th European Symposium on Research in Computer Security*. Egham: Springer.

Jain, M., Tsai, J., Pita, J., Kiekintveld, C., Rathi, S., Ordone, F., & Tambe, M. (2010). Software assistants for randomized patrol planning for the LAX airport police and the federal air marshals service. *Interfaces, 40*(4), 267–290.

Kiekintveld, C., Lisy, V., & Pibil, R. (2015). Game-theoretic foundations for the strategic use of honeypots in network security. In *Cyber warfare* (pp. 81–101). Berlin: Springer.

Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., & Tambe, M. (2011). Stackelberg vs. nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research, 41*, 2011.

Liang, X., & Xiao, Y. (2013). Game theory for network security. *IEEE Communications Surveys and Tutorials, 15*(1), 472–486.

Liu, P., Zang, W., & Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security, 8*(1), 2005.

Matyas, V., & Riha, Z. (2002). Biometric authentication — security and usability. In B. Jerman-Blazic & T. Klobucar (Eds.), *Advanced communications and multimedia security. The International Federation for Information Processing (IFIP)* (Vol. 100). Boston, MA: Springer.

McCarty, B. (2003). The honeynet arms race. *IEEE Security Privacy, 1*(6), 79–82.

McDowell, M. (2009). *Understanding denial-of-service attacks. Security Tip (ST04–015)*. Washington, DC: US-CERT.

Miyachi, T., Narita, H., Yamada, H., & Furuta, H. (2011). Myth and reality on control system security revealed by Stuxnet. In *The Society of Instrument and Control Engineers (SICE) Annual Conference* (pp. 1537–1540). Piscataway, NJ: IEEE.

Moisan, F., & Gonzalez, C. (2017). Security under uncertainty: Adaptive attackers are more challenging to human defenders than random attackers. *Frontiers in Psychology, 8*, 982.

Moore, T., Friedman, A., & Procaccia, A. D. (2010). Would a 'Cyber Warrior' protect us? Exploring trade-offs between attack and defense of information systems. In *Proceedings of the 2010 Workshop on New Security Paradigms* (pp. 85–94). New York: ACM.

Musman, S., & Turner, A. J. (2018). A game oriented approach to minimizing cybersecurity risk. *International Journal of Safety and Security Engineering, 8*(2), 212–222.

Myerson, R. B. (1991). *Game theory: Analysis of conflict*. Cumberland, MD: Harvard University Press.

Nicholson, A., Watson, T., Norris, P., Duffy, A., & Isbell, R. (2012). A taxonomy of technical attribution techniques for cyber attacks. In E. Filiol & R. Erra (Eds.), *Proceedings of the 11th European Conference on Information Warfare and Security* (pp. 188–197). Laval: Academic Conferences & Publishing International Ltd..

NIST. (2002). *Risk management guide for information technology systems* (pp. 800–830). Gaithersburg, MD: NIST Special Publication.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare* (pp. 163–168). Plymouth: Academic.

Pibil, R., Lisy, V., Kiekintveld, C., Bosansky, B., & Pechoucek, M. (2012). Game theoretic model of strategic honeypot selection in computer networks. In J. Grossklags & J. Walrand (Eds.), *Decision and Game Theory for Security. GameSec 2012. Lecture Notes in Computer Science* (pp. 201–220). Heidelberg: Springer.

Podins, K., & Czosseck, C. (2012). A vulnerability-based model of cyber weapons and its implications for cyber conflict. *International Journal of Cyber Warfare and Terrorism, 2*(1), 14–26.

Rasouli, M., Miehling, E., & Teneketzis, D. (2014). A supervisory control approach to dynamic cyber-security. In R. Poovendran & W. Saad (Eds.), *Decision and game theory for security* (pp. 99–117). New York: Springer International Publishing.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computer and Security, 49*, 70–94.

Rowe, N. C., Custy, E. J., & Duong, B. T. (2007). Defending cyberspace with fake honeypots. *Journal of Computers, 2*(2), 25–36.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS), 43*(Part 1), 880–889.

Shamshirband, S., Patel, A., Anuar, N. B., Kiah, M. L. M., & Abraham, A. (2014). Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. *Engineering Applications of Artificial Intelligence, 32*, 228–241.

Shiva, S., Bedi, H., Simmons, C., Fisher, M., & Dharam, R. (2012). A holistic game inspired defense architecture. In *International Conference on Data Engineering and Internet Technology*. Los Alamitos, CA: IEEE.

Sokri, A. (2018). Optimal resource allocation in cyber-security: A game theoretic approach. *Procedia Computer Science, 134*, 283–288.

Tambe, M. (2011). *Security and game theory: Algorithms, deployed systems, lessons learned*. Cambridge: Cambridge University Press.

The American Department of Defence (DoD). (2011). *Cyber Intelligence Preparation of the Environment (CIPE)*. Technical Task Order 11-0002, Version 1.

van Vuuren, J. J., Phahlamohlaka, J., & Leenen, L. (2012). Governance of Cybersecurity in South Africa. In *Proceedings of the 11th European Conference on Information Warfare and Security* (pp. 135–144). Laval: Academic Conferences & Publishing International Ltd..

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for cyber attack attribution*. Alexandria, VA: Institute for Defense Analysis. IDA Paper P-3792.

Zakrzewska, A., & Ferragut, E. (2011). Modeling cyber conflicts using an extended petri net formalism. In *Proceedings of IEEE Symposium on Computational Intelligence in Cyber Security* (pp. 60–67). Piscataway, NJ: IEEE.

Ziolkowski, K. (2010). Computer network operations and the law of armed conflict. *Military Law and Law of War Review, 49*(2), 47–94.