Hausken, Kjell; Welburn, Jonathan William; Zhuang, Jun

Article

A review of attacker-defender games and cyber security

Games

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Hausken, Kjell; Welburn, Jonathan William; Zhuang, Jun (2024) : A review of attacker-defender games and cyber security, Games, ISSN 2073-4336, MDPI, Basel, Vol. 15, Iss. 4, pp. 1-27,
https://doi.org/10.3390/g15040028

This Version is available at:
https://hdl.handle.net/10419/330097

games

MDPI

Review

A Review of Attacker–Defender Games and Cyber Security

Kjell Hausken [1,*], Jonathan W. Welburn [2] and Jun Zhuang [3]

[1] Faculty of Science and Technology, University of Stavanger, 4036 Stavanger, Norway
[2] Pardee RAND Graduate School, 1776 Main St., Santa Monica, CA 90401-3208, USA; jwelburn@rand.org
[3] Department of Industrial and Systems Engineering, University at Buffalo, Buffalo, NY 14260, USA; jzhuang@buffalo.edu
* Correspondence: kjell.hausken@uis.no

Abstract: The focus of this review is the long and broad history of attacker–defender games as a foundation for the narrower and shorter history of cyber security. The purpose is to illustrate the role of game theory in cyber security and which areas have received attention and to indicate future research directions. The methodology uses the search terms game theory, attack, defense, and cyber security in Web of Science, augmented with the authors' knowledge of the field. Games may involve multiple attackers and defenders over multiple periods. Defense involves security screening and inspection, the detection of invaders, jamming, secrecy, and deception. Incomplete information is reviewed due to its inevitable presence in cyber security. The findings pertain to players sharing information weighted against the security investment, influenced by social planning. Attackers stockpile zero-day cyber vulnerabilities. Defenders build deterrent resilient systems. Stochastic cyber security games play a role due to uncertainty and the need to build probabilistic models. Such games can be further developed. Cyber security games based on traffic and transportation are reviewed; they are influenced by the more extensive communication of GPS data. Such games should be extended to comprise air, land, and sea. Finally, cyber security education and board games are reviewed, which play a prominent role.

Keywords: game theory; attack; defense; cyber security

Citation: Hausken, K.; Welburn, J.W.; Zhuang, J. A Review of Attacker–Defender Games and Cyber Security. *Games* **2024**, *15*, 28. https://doi.org/10.3390/g15040028

Academic Editors: Ulrich Berger and Daniel Arce

Received: 26 April 2024
Revised: 26 July 2024
Accepted: 9 August 2024
Published: 14 August 2024

1. Introduction

This article reviews how game theory plays a role in attacker–defender games and cyber security. Cyber security has received increased attention in recent years due to the emergence of the Internet, over which text, voice, and, increasingly, money flow. Players such as firms, organizations, and governments hold, produce, and seek to protect assets and information. The same or other types of players may seek to steal, destroy, or compromise assets and information, either as competitors or with nefarious objectives. This review starts with an overview of attacker–defender games, multiple attackers and defenders, various defense methods, and incomplete information. Having established a foundation in these models, the review proceeds in more detail to cyber security, which typically involves defenders and attackers. Information sharing and security investment are assessed in various circumstances. Models of cyber security stockpiling, deterrence, and resilience are evaluated. Thereafter, reviews are conducted on stochastic games, transportation games, and security education and board games.

Introducing game theory, including attacker–defender games, to cyber security emphasizes how players have different preferences, beliefs, risk attitudes, and strategy sets, which may make the analysis more realistic. The defender seeks to enhance the cyber security of targets that it owns, controls, or operates, while the attacker seeks to compromise this security, e.g., by destroying or stealing targets or broadcasting or falsifying confidential information associated with the targets.

The reviewed articles were identified by using the search terms game theory, attack, defense, and cyber security in Web of Science, supplemented with the authors' knowledge of the field. The research judged to be most impactful was included.

2. This Article's Contribution beyond Earlier Reviews

Table 1 provides an overview of 12 earlier reviews.

Table 1. Overview of 12 earlier reviews.

Reference	Topic	Focus Points
Amin and Johansson [1]	Dynamic games in cyber security	Security and efficiency can conflict. Topics are asymmetric information, evolution of network security, vulnerability assessment, cyber-induced failures, incentives, and design of mechanisms to reduce risks.
Do, et al. [2]	Cyber security and privacy	Applying game theory to cyber–physical security, communication security, survivability, information sharing, software-defined networks, steganography, denial of service, packet forwarding, and privacy. Advantages and limitations from design to implementation of defense mechanisms. Game models, features, and solutions.
Etesami and Basar [3]	Dynamic games in cyber–physical security	Classification of dynamic games into zero sum, stochastic, repeated, differential, Stackelberg, Bayesian, and others. The applications are intrusion detection, risk assessment, signaling games, honeypot/deception, cascading games, Stackelberg security, CBG/hypergame, jamming and eavesdropping, mechanism design, security investment, reinforcement learning, and regret-based learning.
Guikema and Aven [4]	Perspectives on the impact of intelligent attacks on risk	Assessment of the impact of the likelihood of the assumptions of four perspectives of intelligent attacks on risk assessment and management, i.e., game theory, probabilistic risk analysis eliciting probabilities of initiating events from experts, assessing uncertainties beyond probabilities and expected values, and protecting the highest-valued targets while ignoring the attack probabilities.
Hausken [5]	Cyber resilience in firms, organizations, and societies	Cyber resilience involving infrastructure, management, policy, economics, insurance, and Internet of Things. Threat actors and non-threat actors have resources, competence, technology, tools, preferences, and beliefs and make choices. Actors impacting and impacted by cyber resilience are governments, organizations, companies, individuals, insurance companies, cyber security providers, regulators, and threat actors.
Hausken [6]	Defense and attack according to system structure, defense strategies, attack strategies, and defense and attack circumstances	Warfare, methodologies, and defense and attack according to system structure (single target, series systems, parallel systems, series–parallel systems, networks, multiple targets, interdependent systems, degraded systems, dynamically changing system structures, other types of systems), defense strategies (protection, redundancy, deterrence, false targets, separation, individual versus overarching defense and attack, special versus general protection and attack, proactive versus reactive defense, defending with negative or positive incentives), attack strategies (single target, multiple targets, consecutive attacks, random attacks), and defense and attack circumstances (combination of intentional and unintentional impacts, incomplete information, information sharing, cyber war and security, variable resources, expendable versus nonexpendable resources, multiple defenders, multiple attackers, multiple defenders and multiple attackers).
Hausken and Levitin [7]	Defense and attack in reliability systems according to system structure, defense measures, and attack tactics and circumstances	Defense and attack in reliability systems according to system structure (single element, series systems, parallel systems, series–parallel systems, networks, multiple elements, interdependent systems, and other types of systems), defense measures (false targets, separation of system elements, redundancy, protection, multilevel defense, preventive strike), and attack tactics and circumstances (attack against single element, attack against multiple elements, consecutive attacks, random attacks, combination of intentional and unintentional impacts, incomplete information, and variable resources).
Hunt and Zhuang [8]	Attacker–defender games: current state and paths forward	Attacker–defender games with focus on the sequence of moves, number of players, decision variables, objective functions, and time horizons. Relaxing the common assumptions of perfect rationality, risk neutrality, and complete information induces further challenges, e.g., enforcing new assumptions about modeling uncertainties and potential intractability to account for risk preferences. The majority apply methods obtaining closed-form solutions, while the minority apply algorithmic and heuristic approaches. Part of the literature applies data for numerical analysis and computational experiments.

Table 1. *Cont.*

Reference	Topic	Focus Points
Kott, et al. [9]	Six potential cyber game changers	Six potential cyber game changers are that the cyber environment changes in terms of new computing paradigms and new territories for network complexity, new technology trends such as big data analytics and resilient self-adaption, and cybertechnology breakthroughs such as mixed-trust systems and active defenses.
Pala and Zhuang [10]	Information sharing in cyber security	Review of focus and methodology within cyber security information sharing involving firms, governments, citizens, and adversaries. The focus is on the actors involved, types of information shared, current legal baseline, information-sharing organizations/policies/architectures, benefits of sharing, and concerns/costs/barriers of sharing. Qualitative approaches discuss challenges and barriers to public/private collaboration pertaining to privacy and liability to ensure secure and effective sharing. Quantitative approaches balance cyber security investment and information sharing to ensure effective incentives.
Roy, et al. [11]	Cyber security network games	Applying game theory to network cyber security. Their classification taxonomy distinguishes cooperative and non-cooperative games. The latter can be static or dynamic. Static games can have complete or incomplete imperfect information. The latter can be Bayesian or non-Bayesian. Dynamic games can have the four combinations of complete/incomplete and perfect/imperfect information.
Sedjelmaci, et al. [12]	Cyber security games for intelligent transportation systems	Cyber security defense of intelligent transportation systems. Non-cooperative games are divided into interdiction games, mean field games, Stackelberg games, Bayesian games, and zero-sum games. Cooperative Stackelberg games are considered. Cost and security level of these games are assessed as low, medium, or high.

Four of these 12 reviews, i.e., Guikema and Aven [4], Hausken [6], Hausken and Levitin [7], and Hunt and Zhuang [8], focus on attack and defense, with no or tangential reference to cyber security. The remaining eight reviews focus on cyber security from various perspectives. In particular, Amin and Johansson [1] and Etesami and Basar [3] consider dynamic games, Do, Tran, Hong, Kamhoua, Kwiat, Blasch, Ren, Pissinou and Iyengar [2] link to privacy, Hausken [5] links to resilience, Kott, Swami and McDaniel [9] assess future changes, Pala and Zhuang [10] assess information sharing, Roy, Ellis, Shiva, Dasgupta, Shandilya and Wu [11] evaluate network games, and Sedjelmaci, Hadji and Ansari [12] link it to intelligent transportation systems.

This review considers the more recent literature and has, to some extent, a broader focus than the earlier cyber security reviews. More specifically, as shown in Table 2, the review starts with a focus on attack and defense, acknowledging the centrality of intentional intelligent adversaries in cyber security, as opposed to other areas of risk analysis involving nature (weather, etc.) and technology (mechanical failure, etc.). Given this focus, the review proceeds with incomplete information. The defenders may not know who the cyber attackers are; their competences, preferences, and beliefs; and when, how, and who they may attack. The attackers may not know the value of the objects that the defenders protect, which objects are protected, and how they are protected. Since this information can be incomplete, a natural remedy in cyber security is information sharing, considered in Section 6. The remainder of the review delves into more specific areas of cyber security, i.e., stockpiling, deterrence and resilience, stochastic games, education, board games, traffic and transportation, and power systems.

Table 2. Overview of the article.

	Article Section
1	**Introduction**
2	**This Article's Contribution beyond Earlier Reviews**
3	**Defense and Attack**
3.1	*One Player Defending or Attacking One Component in a System*
3.2	*Multiple Attackers and/or Multiple Defenders*

Table 2. *Cont.*

	Article Section
3.3	*Multiple-period Attacker–Defender Games*
4	**Various Characteristics of Defense and Attack**
4.1	*Security Screening and Inspection*
4.2	*Detecting Invaders*
4.3	*Defense through Jamming and Eavesdropping*
5	**Defender–Attacker Games with Incomplete Information**
5.1	*Overview*
5.2	*Protecting ManyTargets*
5.3	*Secrecy and Deception*
5.4	*Threat Propagation, Denial of Service Attacks, and False Alarms*
5.5	*Trust and Reputation*
6	**Information Sharing and Security Investment in Cyber Security**
7	**Cyber Stockpiling, Deterrence, Resilience, and Stackelberg and Repeated Games**
7.1	*Stockpiling of Cyber Munitions*
7.2	*Cyber Deterrence*
7.3	*Cyber Resilience*
7.4	*Cyber Security Stackelberg Games*
7.5	*Cyber Security Games for Power Systems*
8	**Stochastic Cyber Security Games**
9	**Cyber Security Games on Traffic and Transportation**
10	**Cyber Security Education and Board Games**
11	**Strengths, Weaknesses, Opportunities, and Future Research**
12	**Conclusions**

3. Defense and Attack

3.1. One Player Defending or Attacking One Component in a System

One defender and one attacker may defend and attack entire systems or individual components within each system. One example of the latter is the analysis by Hausken [13] of probabilistic risk analysis and game theory. He shows that strategies by individual players at the component level may impact the risk at the system level. For example, consider a series system, e.g., a circular island where each citizen owns a wedge-shaped slice. To avoid flooding, each citizen may build a dike. Flooding may occur through the lowest dike, which is the weakest link. One Nash equilibrium, if dikes are expensive or flooding is unlikely, is that no citizens build dikes. A second Nash equilibrium is that all citizens build dikes. Next, consider a parallel system, e.g., multiple antimissile batteries, each controlled by one player, firing at an incoming missile against a city. It suffices that one antimissile battery can shoot down the incoming missile. One Nash equilibrium, if shooting down a missile is expensive, is that no player shoots down the missile. Additional Nash equilibria consist of one of the players shooting down the missile, which constitutes both a battle of the sexes game and a chicken game. The player that shoots down the missile earns lower utility than the other player(s). Next, consider a summation game, e.g., multiple companies that may or may not aid each other. If aiding is very expensive, no company will aid in a mutual defection game. If aiding is very expensive, no company will aid in a mutual defection game. If aiding is intermediately expensive, no company

will aid in a prisoner's dilemma. If aiding is not expensive, all companies aid in a mutual cooperation game. Hausken [13] further analyzes combined series and parallel systems.

3.2. Multiple Attackers and/or Multiple Defenders

Although most of the literature studies a single attacker and a single defender, in reality, there could be multiple attackers interacting with multiple defenders. Ackerman, et al. [14] study the potential collaboration among multiple extremist groups from diverse milieus, despite significant ideological disparities, to align to a certain extent, enabling operational collaboration against Western societies. Xu and Zhuang [15] study a sequential one-defender–N-attacker game where N attackers are treated as independent agents. On the defender side, Zhuang, et al. [16] and Zhuang [17] study an interdependent security problem where multiple defenders are connected in a network but make security investment decisions under different discount rates.

Combining multiple attackers and multiple defenders, Shan and Zhuang [18] study the unique problem of subsidizing to disrupt a terrorism supply chain involving multiple governments and multiple terrorist groups. They first study two subgames: a proliferation game between terrorist groups and a subsidization game between governments. They then integrate these two subgames to study how the victim government can strategically use subsidies to incentivize the host government to disrupt the terrorism supply chain.

3.3. Multiple-Period Attacker–Defender Games

Researchers have also studied scenarios where an attacker and a defender interact over multiple periods. For example, Hausken and Zhuang [19] study a T-period game where both the attacker and the defender attack and defend, considering different scenarios, such as changing resources, the random determination of resources, and the impact of previous attacks on future resource allocation. Several interesting strategies are then studied in a multiple-period game setting, including terrorists who accumulate or stockpile resources [20–22] and terrorists who choose in which period to attack and could be deterred [23]. Note that, within each period, most works study either a simultaneous-move or a sequential-move two-stage game (where the defender typically moves first). However, some works also study multiple-stage games, e.g., such that retaliation may occur in the third stage; see Shan and Zhuang [24].

4. Various Characteristics of Defense and Attack

Three common characteristics are security screening and inspection, detecting invaders, and defense through jamming.

4.1. Security Screening and Inspection

One specific attacker–defender game involves security screening and inspection in the context of airport security, visa approval, and cargo container inspections. The defender sets a probability of screening when facing an adaptive attacker who decides whether to attack or not. Wang and Zhuang [25] study the balance of congestion and security among three groups of players with incomplete information. These are a defender who sets the probability of screening, an attacker who decides whether to attack, and a group of normal applicants who decide whether to join the queue. Extending their work, studies have been performed on a two-stage [26] and N-stage [27] security screening problem with screening errors, a parallel-queue security screening problem with incomplete information [28], and impatient applicants [29]. Haphuriwat, et al. [30] assess how to deter the smuggling of nuclear weapons in container freight through detection and retaliation. They find that unless the defender imposes high retaliation costs, 100% inspection is likely needed, and deterrence with partial inspection may be challenging. However, when the attacker can be credibly threatened with costly retaliation, partial inspection may be sufficient to deter nuclear smuggling attempts. Brown, et al. [31] develop a max–min project management critical path method considering how to interdict a nuclear weapons project. The prolifer-

ator seeks to complete a batch of fission weapons quickly, while the interdictor seeks to delay indefinitely. They consider three uranium enrichment technologies that all involve cascade loading, causing fragility for the proliferator. This, in turn, enables the interdictor to intervene diplomatically, economically, and militarily.

4.2. Detecting Invaders

Detecting invaders is a challenge. Assessing detection at sea, Gerald, et al. [32] develop a defender–attacker model considering how to position patrol vessels optimally to detect an adversary in speedboat(s) seeking to evade detection (e.g., through elevated obstructions) while attacking. The vessels have a surface search radar, radios, and a machine gun. Alert defenders are almost guaranteed to detect attackers by optimal prepositioning, accounting for bottlenecks and the restricted navigational access channels to ports. They sometimes recommend positioning far from bottlenecks to better detect stealthy evading attackers. Assessing how to defend an oceanic bastion against submarine attacks, Brown, et al. [33] present a two-person zero-sum game for the application of ships, aircraft, etc., in defense. The attacker knows the ship locations but not where the other defense platforms are located. The attacker chooses a path towards the bastion, while the defender maximizes the detection probability. Considering detection more generally, Orojloo and Azgomi [34] develop a game for each of the two phases of intrusion and disruption by an attacker of a cyber–physical system. The attacker seeks to understand the system's failure conditions, control principles, and signal processing. The system evolves continuously between different states according to ordinary differential equations. They estimate the system's security according to metrics, e.g., availability and mean time to system shutdown, and exemplify with a chemical plant.

4.3. Defense through Jamming and Eavesdropping

Jamming is another common defense method. Focusing on a wireless mesh network that enables data, voice, and video communication, Nicholas and Alderson [35] develop a defender–attacker–defender model for its design, attack, and operation. The defender uses radio propagation over terrain downloaded from the Internet and minimizes the worst possible disruption that an adversary can inflict through jamming, i.e., electromagnetic interference. Jamming can be combined with eavesdropping. Xu, et al. [36] consider various games within mobile communication technologies and the commercial use of 5G, including eavesdropping and anti-eavesdropping and jamming and anti-jamming. They assess potential research directions. Xu and Baykal-Gursoy [37] consider a non-zero-sum game for the defense of a wireless communication network of channels through jamming an adversarial eavesdropper. When the eavesdropper attacks all of the channels, they solve a convex optimization problem. Otherwise, the eavesdropper selects channels probabilistically, which impacts the defender's defense. A unique Nash equilibrium is obtainable under certain conditions. A strategy iteration algorithm determines an equilibrium power allocation strategy that outperforms assuming that every channel is under attack. Finally, a stochastic approach is presented by Garnaev, et al. [38]. They develop stochastic communication games where a user chooses optimally whether to transmit, which may lead the adversary to jam or delay the transmission, which may enable the detection of the adversary if it continues actively to jam instead of eavesdropping passively. The adversary may find eavesdropping less efficient if it cannot time-efficiently utilize the compiled information. They find that incorporating a detection time slot in the transmission may improve the communication reliability and secrecy.

5. Defender–Attacker Games with Incomplete Information

5.1. Overview

Complete information is the starting point for most analyses. Research on incomplete information in defense and attack has been conducted by Nikoofal and Zhuang [39], Zhuang and Bier [40,41],Zhuang, et al. [42],Dighe, et al. [43]; Wang and Bier [44,45]; Song and Zhuang [28]; Zhai, et al. [46]; and Dong, et al. [47]. Research on incomplete

information within adversarial risk analysis has been conducted by Rios Insua, et al. [48], Rios Insua, et al. [49]; Rothschild, et al. [50]; and Banks, et al. [51].

5.2. Protecting Many Targets

The protection of many targets is analyzed by Bier [52]. She considers how a defender allocates resources to protect many targets against an attacker with unknown preferences who chooses one target to attack and observes the defender's resource allocation. The increased defense of one target decreases the attack probability against this target. Some targets may optimally be left undefended. Higher vulnerability at one target may be optimal, even if lower vulnerability could be achieved at zero cost. The defender prefers centralized allocation. A larger number of targets to defend requires the number of valuable targets to be bounded for the defender to cost-effectively decrease the attack success probability. The optimal resource allocation can be nonmonotonic in how the attacker relatively values the outside option. The defender prefers its allocation to be public. Various extensions of this work have been presented. First, Bier, et al. [53] consider how to protect against an unknown attacker, assuming that the attack success probability depends on how the defense resources are allocated and that the attacker can be of as many unknown types as the number of assets attacked. Second, Hausken [54] assumes that the attacker's resources and target valuations are drawn probabilistically and that the attack success probability depends on how the defense and attack resources are allocated. More specifically, in a two-period game where the defender moves first and the attacker moves second, which asset is attacked depends on the attacker's type, the unit attack costs, the contest intensity, and the defense. An interior equilibrium for two equivalent assets exists for a low contest intensity. A corner equilibrium with no defense exists for a high contest intensity when the attacker is resourceful. The isoutility curves can be both upward-sloping (the defender prefers to invest less in defense) and downward-sloping (e.g., when one asset has a low value or high unit defense cost), which contrasts with the work of Bier, Oliveros and Samuelson [53], finding upward-sloping isodamage curves near the axes. In other words, the defender prefers to invest less, which increases the probability of successful attacks on both assets. Finally, Yolmeh and Baykal-Gürsoy [55] consider a simultaneous game with an unknown distribution of information about the target values and detection probabilities. The attacker maximizes the damage or infiltrates multiple targets that the defender defends. They determine the existence and uniqueness of a Nash equilibrium for two games and the shape of the Nash equilibrium for the third game. He and Zhuang [56] study the possibility of contracts or mutually beneficial arrangements between a government and a terrorist group using a sequential game framework. Equilibrium solutions are derived for models with complete and incomplete information, revealing that successful contracts can potentially deter attacks and increase the payoffs for both the government and certain types of terrorist groups, providing new insights into counterterrorism strategies.

5.3. Secrecy and Deception

Most of the literature assumes that the information disclosed in the attacker–defender game is truthful, e.g., the second mover is able to perfectly observe the first mover's decision and then respond accordingly. However, in reality, some information may be kept secret (Dighe et al., 2009) or even deceptive, leading the other players to potentially learn the truth [57]. Zhuang and Bier [58] show that truthful disclosure is preferred in games of complete information. Zhuang and Bier [40] and Zhuang, Bier and Alagoz [42] use a Bayesian Nash equilibrium approach to study secrecy and deception, where the defender sends a signal that is different from what the defender actually does. Zhuang and Bier [41] summarize the potential reasons for secrecy and deception in homeland security resource allocation games. Hunt, et al. [59] study disclosure and secrecy using a signaling game in the context of technology adoption for airport security.

5.4. Threat Propagation, Denial of Service Attacks, and False Alarms

Threat propagation is analyzed by Liu, et al. [60]. They observe that attackers in distributed cyber–physical systems tend to initiate attacks in the outer nodes and proceed towards the inner nodes, hoping not to be detected. Defining the weighted colored Petri net, the authors model threat propagation between nodes as a mixed-strategy Bayesian attack–defense incomplete information game. They determine the Bayesian Nash equilibrium, threat propagation matrix, and security state vector to determine the attack paths and losses. Denial of service attacks are investigated by Gupta, et al. [61]. In a zero-sum game, they determine the saddle-point equilibrium. More generally, they develop an asymmetric information non-zero-sum game between an attacker and a cyber–physical system controller. Assuming resource-constrained players, an algorithm determines a subclass of Nash equilibria. Some of the research considers the role of false alarms. Han and Choi [62] present a dynamic game where a defender is penalized for false alarms in a cyber security intrusion detection system. They find that the demand and supply of cyber insurance can be low and that decreasing the operational risk decreases the cyber risks and increases the false alarm rate. They recommend a government intervention policy, which implies a socially optimal outcome.

5.5. Trust and Reputation

Trust and reputation often play a role in incomplete information games. Trust and reputation are linked since a reputable player more likely earns the trust of other players. Njilla, et al. [63] consider a cyberspace game where service providers seek to maintain a reputation that ensures economic gains, the users prefer to trust the service providers, and attackers seek to breach a provider's database and expose the users' private information. They recommend that service providers should invest in cyber security. Han and Choi [64] consider a reputation game where an attacker can pretend to be a normal user. The defender may have to announce that it has been attacked without knowing whether it has been attacked. They demonstrate a sequential equilibrium's existence and uniqueness in Markov strategies and propose empirically and theoretically how to calibrate the attack probability.

6. Information Sharing and Security Investment in Cyber Security

In risk analysis, information is often dispersed differently across players. This problematizes whether players have incentives to share information strategically. Gordon, et al. [65] assess the cost-side effects regarding how information sharing impacts information security. They illustrate how underinvestment in security may follow from a tradeoff between information security investment and free-riding. Gal-Or and Ghose [66] analyze the demand-side effects of economic incentives for information. They show that security investment and information sharing are strategic complements, while Hausken [67] shows that they are strategic substitutes. Hausken [67] finds that information sharing between firms is inversely U-shaped in an attack. He models information sharing across connected firms, finding that firms tend to underinvest and free-ride unless a single well-respected social planner moves first and coordinates sharing. He shows that individual optimization implies free-riding, which can be curtailed by a social planner. If the social planner moves simultaneously with the firms, it imposes unreasonably high sharing. If the social planner moves before the firms, it imposes reasonable sharing.

For a simultaneous move game, Hausken [68] finds that two hackers free-ride on each other's information sharing when attacking one firm. Each hacker's attack and information sharing are strategic complements, while one hacker's attack and the other hacker's information sharing are strategic substitutes. Hausken [69] analyzes information sharing between two attackers attacking one firm in a four-period game, firm-hacker 1-firm-hacker 2. Hacker 1′s information sharing increases both hackers' focus on reputation gains. Hacker 2′s attack is deterred by hacker 1′s focus on reputation gains.

Generalization to a similar four-period game with an attack on two firms is described by Hausken [70]. Two hackers share information. Two firms share information. If hacker 2

is disadvantaged in some way, it receives less information from hacker 1. Mixed motives may exist between information sharing and reputation gains. Hacker 2′s attack is deterred by the first hacker's reputation gain. Increased interdependence between firms causes more information sharing between hackers. The firms deter disadvantaged hackers. Increasing information-sharing effectiveness causes firms to substitute from defense to information sharing with each other.

Four four-period games where one firm defends proactively or retroactively against hacker 1, and thereafter against hacker 2, are analyzed by Hausken [71]. Hacker 1′s attack and information sharing are strategic substitutes. Various results are developed. For example, when the firm is proactive in period 1, hacker 1′s information sharing decreases with hacker 2′s attack cost. The firm's deterring effort in eight corner solutions is proportional to the deterred hacker's valuation and inversely proportional to the deterred hacker's unit effort cost. When hacker 1 exerts higher effort and shares more information, lower defense by the firm is sufficient to deter hacker 2. The results contrast the literature where the advantaged player commonly prefers to move first.

In the context of cyber security information sharing, He, et al. [72] provide a decision-theoretic approach, discussing various information-sharing structures, strategic interactions between stakeholders, costs, benefits, and the mechanism of information sharing to enhance the understanding and provide a detailed cost–benefit analysis of this public–private partnership. Pala and Zhuang [10] examine the literature on cyber security information sharing and explore considerations of various stakeholders, including firms, governments, citizens, and adversaries. They highlight the prevalence of both qualitative and quantitative approaches, with quantitative approaches addressing challenges in public–private collaboration and proposing game-theoretic secure sharing mechanisms. Levitin, et al. [73] assess how a defender stores information to prevent an attacker from stealing or destroying it. The defender, either minimizing the probabilities of information detection and data theft or minimizing the cost, allocates information to multiple blocks and maximizes the number of copies of each block subject to resource constraints.

Tosh, et al. [74] present an evolutionary game where organizations share cyber security information to ameliorate cyber attacks against critical resources. They account for a dynamic cost adaptation scheme, a distributed learning heuristic. The economic benefits of information sharing are assessed, together with the consequences of not taking part in the game.

Many have sought to understand the role of cyber security investment in games of firms interconnected and interdependent in communication and supply chain networks. In many of these games, firms face the potential to suffer a cyber attack (or breach) directly or indirectly through shared network ties and must choose their levels of investment and information sharing. For example, Bandyopadhyay, et al. [75] present a model of firms interconnected in supply chain and communication networks, finding that the security investment depends on the nature of the dependence. They find that when firms are connected through communication networks alone, they are incentivized to underinvest and free-ride. In contrast, when firms are connected through both communication networks and supply chains (i.e., production, ownership, or financial ties), they are incentivized to increase their investment when tightly integrated and decrease their investment when they are loosely integrated. Nagurney, et al. [76] model retailers and customers connected in a supply chain, finding that increased interdependence can increase the vulnerability to an attack.

In a multiform model of investment, Nagurney and Shukla [77] find that information sharing leads to both financial and security benefits. Simon and Omar [78] present a model of a supply chain with multiple defenders (one at each node) and a single attacker. They model attackers as either non-strategic (random attacks) or strategic (adaptive adversary) and defenders as either uncoordinated or coordinated. They find that the security investment is suboptimal in the absence of coordination. Finally, Li and Xu [79] discuss overcoming the prisoners' dilemma and free-riding challenges in a supply chain game

through coordination mechanisms including joint decision-making, risk competition, and information sharing. They find that joint decision-making and security risk compensation are preferable to stimulate firms' investments and decrease costs compared with security information sharing.

7. Cyber Stockpiling, Deterrence, Resilience, and Stackelberg and Repeated Games

7.1. Stockpiling of Cyber Munitions

The majority of the literature seeks to better understand defensive strategies; see, e.g., Alpcan and Basar [80], Acemoglu, et al. [81], and Kovenock and Roberson [82]. A small amount of the literature seeks to understand the behavior of cyber attackers, including the stockpiling of zero-day cyber vulnerabilities. For example, Wang, et al. [83] develop a two-period game-theoretic model of zero-day attacks with stockpiling. In period 1, one player produces zero-day exploits for immediate deployment or stockpiling. In period 2, the same player repeats this procedure, supplemented with stockpiling from period 1. The other player defends in both periods. They show that the first player stockpiles when its unit effort cost of producing zero-day exploits is lower in period 1. It may even accept negative expected utility in period 1 if it is compensated in period 2. With a higher contest intensity in period 2, the players compete more fiercely with each other in both periods. Hausken and Welburn [84] consider a cyber war where two players produce zero-day cyber exploits allocated in a cyber attack and stockpiling and defend against attacks. Each player's utility is inversely U-shaped in each player's unit defense cost. Higher contest intensities cause higher effort until the players' resources are fully exploited and they receive zero expected utility. Lower Cobb–Douglas output elasticity for a player's stockpiling of zero days causes higher attack and expected utility, which eventually reaches a maximum; this is detrimental for the opposing player. Schramm, et al. [85] consider a zero-sum game where each player decides if and when to use a munition based on a cyber exploit discovered according to an independent random process. Each player's payoff increases if it postpones exercising the munition, which matures, but receives zero payoff if the opposing player also discovers the munition. They determine the optimal munition exercise strategies and quantify the value of cyber conflicts.

7.2. Cyber Deterrence

Others have used game theory, often leveraging the foundational game-theoretic work of Schelling [86], Dresher [87], and others, along with strategic discussions of cyber deterrence (e.g., Libicki [88], Nye [89], Crosston [90], Jensen [91], Clarke and Knake [92], Jasper [93]), to study the ability to defend against and deter cyber attacks. Edwards, et al. [94] introduce an attribution game in a defender–attacker setting where defenders are uncertain about the ability to attribute an attack to an attacker (the attribution problem). Baliga, et al. [95] advance the attribution game in a model with a single defender, multiple attackers, and uncertain attribution. Baliga, De Mesquita and Wolitzky [95] find that more frequent attacks from any given attackers increases their likelihood of successful attribution relative to others, which results in endogenous complimentary among attackers, where attackers are only as aggressive as the most aggressive attacker and not more. Moreover, Welburn, et al. [96] present a model between a defender and a cyber attacker with imperfect attribution, where the defender also can signal its capability to retaliate against an attack. They find the presence of equilibria where deterrence is achievable through signaling, while, in a counterintuitive case, defenders may be able to increase their rewards by luring weak attackers.

7.3. Cyber Resilience

Assessing cyber resilience in firms, organizations, and societies, Hausken [5] considers threat actors and non-threat actors nested inside each other. They possess competence, resources, technology, and tools. They choose strategies based on their preferences and beliefs, which influence and are influenced by cyber resilience. Cyber resilience relates to

the Internet of Things, where artificial intelligence, machine learning, and robotics play increasing roles. Vulnerabilities may follow from possible excessive trust in computers and software, inadequate data handling, deficient technology, and too many attack surfaces. Cyber resilience also relates to cyber insurance due to cover limitations, preconditions or entry requirements for cyber contracts, data compilation, and the handling of incident responses. Zhu and Basar [97] discuss game-theoretic methods for the robustness, security, and resilience of cyber–physical control systems. They distinguish between robust, adaptive, and stochastic control, to address vulnerabilities within these frequently open networks. Backhaus, et al. [98] consider designs of attack-resilient smart grids and control systems, accounting game-theoretically for machine-mediated human–human interactions. They assess outcomes via simulations and consider how to develop tools to defend against a cyber–physical intruder.

7.4. Cyber Security Stackelberg Games

A few cyber security Stackelberg games have been identified. First, Zhang and Malacaria [99] apply mixed-integer conic programming to develop optimal cyber security controls against multi-stage attacks. They use preventive optimization, a learning mechanism, and online optimization, shown to be a Bayesian Stackelberg game solution and more efficient than, e.g., the Harsanyi transformation. Second, Shukla, et al. [100] develop a zero-sum, two-player Stackelberg game where a sufficiently resourceful defender protects a networked control system of nodes robustly against a budget-constrained cyber attacker. They solve this with backward induction and exemplify with electric power systems. Third, Shen and Feng [101] present a Stackelberg interdependent security game between individual self-interested non-malicious cyber–physical systems that are vulnerable due to their distributed and hierarchical nature. They determine pure strategy equilibria and the strategy gap between the individual and social optimum.

7.5. Cyber Security Games for Power Systems

Two cyber games have been identified for power systems. First, Gao and Shi [102] present a three-stage defender–attacker–defender game for cyber–physical power systems. They account for the operation risks and vulnerabilities of transmission lines. To mitigate attacks, they incorporate the time delay of system recovery and distributed denial of service and apply the particle swarm optimization approach and sequential quadratic programming. The approach is validated through two case studies. Second, Li, et al. [103] develop a graphical evolutionary game as competition between virus propagation and countermeasures to protect cyber nodes within power systems. Each node plays as a defender or an attacker according to its state. Probabilistic strategies and state transfers depend on a death–birth rule, which dynamically impacts the infection probability of each substation over time.

8. Stochastic Cyber Security Games

The relevance of incomplete information and uncertainty in cyber security suggests the relevance of stochastic analysis. Hence, as expected, several stochastic cyber security approaches have been proposed, as shown in Table 3.

Eight of the 12 games in Table 3 assume one defender and one attacker, covering phenomena such as intrusion detection, jamming and eavesdropping, and one epidemic model. The remaining four games model multiple players—typically multiple defenders—and, in two models, also multiple attackers. Two models assume bounded rationality. Two of the models apply mean-field theory. Mean-field game theory intersects game theory, stochastic analysis, and control theory. Each player plays against a field of players, which can be realistic for many players, so that a representative player for the field can be identified. It is inspired by mean-field theory in physics, where individual particles, among many particles, impact the system negligibly.

Table 3. Stochastic approaches to cyber security.

Reference	Players	Assumptions	Methods	Results
Alpcan and Basar [80]	One defender, one attacker	An intrusion detection system allocates resources for detection and response, limited information, Q-learning	Stochastic network intrusion detection as a finite Markov chain	Analyze the outcomes and evolution of an example game numerically for various game parameters
Garnaev, Baykal-Gursoy and Poor [38]	One defender, one attacker	A user as a defender chooses optimally whether to transmit, which may lead the adversary to jam or delay the transmission, which may enable the detection of the adversary if it continues to actively jam instead of eavesdropping passively	Stochastic communication subject to jamming and eavesdropping	The adversary may find eavesdropping less efficient if it cannot time-efficiently utilize the compiled information, and incorporating a detection time slot into the transmission may improve the communication reliability and secrecy
Hu, et al. [104]	One defender, one attacker	Acknowledge today's presence of firewalls, intrusion detection, and cryptography, but emphasize the need for a strategic focus	Stochastic evolution of cyber security applying the logit quantal response dynamics equation to specify the cognitive differences of real-world players	Determine the defense cost and benefit, exemplified with ransomware studies
Huang, et al. [105]	One defender, one attacker	Time-based unified payoff quantification	Quantitative vulnerability analysis to build a cross-layer stochastic security game in an industrial cyber–physical system	Presentation of a hardware-in-the-loop simulation testbed case study
Kolokoltsov and Bensoussan [106]	Multiple defenders (computer owners as customers), one hacker	The computer owners are offered various defense systems, where the infection controlled by the botnet herder propagates as a random process	Mean-field stochastic game analysis of cyber security	The stationary version is solved given that the customers' execution time is much faster than the infection rate
Miao and Li [107]	Multiple defenders, multiple attackers	Binary interaction between attackers and defenders and stochastic propagation of infected computers in a network	Susceptible–infected–removal epidemic mean-field stochastic cyber security analysis	Formulation of the consistency stability problem generated by a Hamilton–Jacobi–Bellman equation
Miao, et al. [108]	One defender, one attacker	A strategy is to combine one controller, one estimator, and one detector among the candidate components at each state	Hybrid zero-sum stochastic finite horizon analysis of cyber–physical system with a value iteration algorithm with an upper bound for the value of the finite horizon game	Scalable and real-time computation of switching strategies to balance the security overhead and control cost
Miao, et al. [109]	Multiple defenders, multiple attackers	Each defender has discrete-time dynamics and balances the individual cost against the overall network cost	Mean-field cyber security analysis in Hilbert space where infinitely many players cause a Nash equilibrium for the individual cost function	An optimal condition is determined where the equilibrium is the optimal solution to the overall cost function, illustrated with numerical examples
Orojloo and Azgomi [110]	One defender, one attacker	Distinguishing two phases, i.e., an intrusion process and a disruption process	Stochastic game of a cyber–physical system	Nash equilibria, best response strategies, and mean time to shutdown are determined, illustrated with a boiling water power plant

Table 3. *Cont.*

Reference	Players	Assumptions	Methods	Results
Singh, et al. [111]	One defender, one attacker	Bounded rationality that restricts to a stateless stochastic game where a defender learns the attacker's cyber behavior	Stochastic online cyber security with incomplete information, criticizing state-oriented Markov games where the number of states explodes	The approach compares favorably with other approaches regarding convergence and the simulation time span
Xing, et al. [112]	Players are multiple sensors deciding whether to invest in security when sending data packets	The security of the sensors is interdependent due to the network-induced risks and shared over a communication network	Stochastic non-zero-sum games with asymmetric information between resource-constrained players in cyber–physical systems	Develop a backward induction algorithm to determine the Nash equilibria
Zhang and Liu [113]	One defender, one attacker	Bounded rationality to handle the many possible states in networks with many nodes	Stochastic analysis of cyber security where the defender's decision algorithm applies time-efficient online learning	The strategy is superior to previous evolutionary equilibrium strategies because it does not rely on prior data

9. Cyber Security Games on Traffic and Transportation

Table 4 shows cyber security games on traffic and transportation.

Table 4. Cyber security games on traffic and transportation.

Reference	Game	Assumptions	Methods	Results
Huo, et al. [114]	Vehicular cyber–physical coalition formation game where vehicles are nodes switching between coalitions	The coalition utility depends on the relative velocity, position, and bandwidth availability ratio of vehicles in a cluster	Address the overload and low communication efficiency, introducing a reputation-based incentive and penalty mechanism	Convergence to a Nash-stable partition is possible, preventing selfish nodes from entering clusters
Sanjab, et al. [115]	One interdictor targeting one unmanned aerial vehicle operator	Interdictor can be benign or malicious	They apply prospect theory and account for subjective valuations and risk perceptions for equilibrium determination	The interdictor chooses the optimal location(s) for targeting, while the operator chooses the optimal path to evade attacks and minimize the mission completion time
Sedjelmaci, et al. [116]	Hierarchical vehicular network game between two types of collaborating players	An intrusion decision agent is a head player, supported by secondary agents	The secondary agents cooperate to detect, predict, and react to cyber attacks	They ensure low communication overhead and low delay to obtain low false positive and false negative rates compared with alternative approaches
Sedjelmaci, Hadji and Ansari [12]	Multiple players in intelligent transportation systems	Cyber security Stackelberg game	Evaluation of suitable security levels and costs and survey of defense methods	They identify an attack's characteristics to enhance the detection efficiency
Wu, et al. [117]	Non-cooperative incomplete information dynamic Bayesian game between air traffic management and one attacker	The attacker may camouflage its attack type when attacking a cyber–physical system	Air traffic management may detect the attack type with a certain probability	They determine the perfect Bayesian Nash equilibrium and its existence conditions, enabling the defender to decrease the system loss
Yang, et al. [118]	Bayesian game between an attacker and a defender of a coupled transportation network and a cyber–physical power system	They account for the load shedding loss of load buses	They simulate the travel of electric vehicles potentially impacted by charging station outages	Experiments are conducted to confirm the model's effectiveness

Traffic and transportation occur in the air, on land, and at sea; may or may not involve humans; and may or may not involve transported goods. At present, the emergence of self-driving or driverless vehicles is prominent; they require the wireless communication of a plethora of data across multiple vehicles and data centers. Examples of data are the GPS coordinates, speed, direction, size, and types of other vehicles and non-vehicles, as well as the geography, weather, road conditions, laws and regulations, etc. Similar types of communication occur or may occur between units in the air or at sea and in air/sea/land traffic management. Such communication inevitably invokes cyber security, where both benevolent and non-benevolent players seek to obtain their objectives according to their beliefs.

10. Cyber Security Education and Board Games

The advances of computer technology have facilitated the simulation of cyber security phenomena. This may explain the emergence of games to facilitate learning, training, education, and awareness about cyber security. Some of these games are board games, tabletop games, card games, and experimental games; see Table 5.

Table 5. Education and board games.

Reference	Game	Objectives	Methods	Results
Cone, et al. [119]	Interactive video game	Build security awareness and support organizational security training in an engaging security adventure	The game applies security concepts and is designed to address organizational cyber security requirements and policies	The game is successfully utilized for information assurance education and may facilitate information awareness
Frey, et al. [120]	Tabletop game	Players can experiment, learn and reflect over security risks and identify decision patterns, including good practices, typical errors, and pitfalls	Players' decision-making processes are classified as driven by procedure, experience, scenario, or intuition	Managers and security experts generally favor technological solutions, computer scientists prefer personnel training, and security experts are more confident but may make questionable decisions
Futter [121]	War games	Analysis of cyberthreats, nuclear security, and arms control deemed especially relevant for USA–Russia relations	Analysis of strategic instability, perceived safety, miscalculation, potential unauthorized nuclear use, and possible future nuclear cuts	Assessments are performed of the many nuclear weapons on hair-trigger alert, where vulnerabilities and problems are potentially exploitable by third parties
Harta, et al. [122]	Tabletop game	Educate and build cyber security awareness, complementing instruction-led or computer-based security training	Players play as attackers or defenders of critical assets in a fictitious organization	Players acquire knowledge, security awareness, and education on cyber security
Jin, et al. [123]	Zero-sum game	Denial of service analysis in a cyber–physical system with a sensor as a defender and an attacker	Dynamic adjustment of reinforcement learning algorithm	The players' strategies converge to the Nash equilibrium
Kanellopoulos and Vamvoudakis [124]	Dynamic security game	Presentation of a learning algorithm to train the different intelligence levels for boundedly rational agents with level-k intelligence	Development of an iterative method of optimal responses in a cognitive hierarchy cyber–physical system	Equilibrium stability of the closed-loop system and convergence to the Nash equilibrium when the intelligence level approaches infinity

Table 5. *Cont.*

Reference	Game	Objectives	Methods	Results
Maqbool, et al. [125]	Laboratory experimental game	Determine the monetary consequences of cyber attacks on the decision-making of defenders	Random assignment of participants as multiple hackers or multiple defenders	Penalizing defenders for false alarms or misses is 10 times costlier for the defenders than equal payoffs; participants rely excessively on recency, frequency, and variability
Nicho [126]	Education game	Build cyber security awareness and decrease user vulnerabilities	Train organizational users	Detect, prevent, eliminate, mitigate, and report social engineering threats generated by advanced persistent threat vectors
O'Connor, et al. [127]	Training game for cyber security	Applying the conceptual framework for e-learning and training as a pattern for designing a serious game	Using a simulated critical infrastructure protection scenario platform, developed in collaboration with industrial partners	Running different scenarios involving financial forecasting and protecting infrastructure such as electricity generation plants
Ravishankar, et al. [128]	Software cyber warfare testbed game	Analysis of a game between multiple attackers and multiple defenders of critical infrastructure	Using a probability and belief function to account for strengths, vulnerabilities, and uncertainties of information	Optimal strategies are determined and validated using simulation experiments
Shah and Agarwal [129]	Card game	Increase smartphone security awareness	Application of constructive learning theory and the Fogg behavior model, evaluated with a between-subjects design	Participants in the intervention group are 2.65 times more likely to adopt the recommended behavior
Tseng, et al. [130]	Board game	Cyber security education and learning with an attack and defense knowledge self-evolving algorithm and a gaming portfolio mining procedure, tested in a children's summer camp	An ontology fusion-or-splitting procedure for collected cyber security incidents and a quasi-experiment of pre/post testing and concept map testing	Experiments show that students can better acquire up-to-date cyber security knowledge and learn more effectively than in traditional classrooms
Yamin, et al. [131]	Training game	Continuous training and self-learning of cyber security skills	Players are attackers or defenders, making real-time cyber security decisions	Cyber security exercise scenarios are developed and simulated
Yasin, et al. [132]	Education game	Learn about cyber security to motivate and enable learning about security attacks and vulnerabilities	Application of cyber security knowledge and empirical evaluation, literature review	The approach reflects real life in a presentable and understandable way
Zeijlemaker, et al. [133]	Board game	Development of a game that reflects the real-life environment of bank managers	Design of support tools that capture the complex, dynamic nature of cyber security decisions	Poorly performing decision-makers may be unaware of their poor performance and employ heuristics, causing misguided decisions involving overreaction rather than proactivity

11. Strengths, Weaknesses, Opportunities, and Future Research

This review distinguishes itself from the earlier 12 reviews listed in Table 1 by incorporating more recent research and by starting with the longer and broader history of attacker–defender games, before proceeding with the shorter and narrower history of cyber security. The study of cyber security brings the need to review incomplete information and information sharing, followed by cyber stockpiling, deterrence, resilience, and stochastic analyses. Thereafter, two phenomena in which cyber security is essential are reviewed:

traffic and transportation impacted, for example, by the communication of GPS data—e.g., between self-driving cars—and education and board games facilitated by the increasing use of computers and electronic devices.

Table A1 in Appendix A shows the players and phenomena considered in the reviewed articles. Fifty-seven of the 132 works involve one defender and one attacker, which is a common game-theoretic approach, while the others involve multiple players in various constellations. Future research may assess each phenomenon involving one defender and one attacker to determine whether more players can be introduced to obtain more realistic analyses. Similarly, some of the research with multiple players may remove or introduce players to realistically capture phenomena. Table 3 shows the players, assumptions, methods, and results of stochastic analyses of cyber security. Table 4 shows the game assumptions, methods, and results of cyber security games on traffic and transportation. Table 5 shows the game objectives, methods, and results for education and board games. These three tables provide a strong basis for the assessment of alternative phenomena, different constellations of players, different assumptions, and different games and methods, which may yield different results. Several of the models are in need of empirical validation to ensure that they meet societal needs.

Players in the literature commonly value targets subjectively along one dimension, which is challenging for targets of different types, which may differ in their economic, human, and symbolic value. Future research may value targets along multiple dimensions. To the extent that targets are not clearly distinguishable, they may be aggregated into distinguishable clusters, applying Simon's [134] principle of "near decomposability". The same applies for players that may have partly aligned preferences or beliefs, which may be aggregated into unitary players with preferences or beliefs approximating those of their constituent players. Future research should assess which players and targets are relevant to include in the analysis, which games they play, in which sequences the players move, whether the information is incomplete or uncertain, and whether the players are fully or boundedly rational, adjusted towards societal needs for an enhanced understanding.

Common methodologies in the reviewed literature, in addition to game-theoretic analyses implying, e.g., equilibria and min–max solutions, are simulations applying various algorithms, probability theory, and stochastic analysis. Future research may apply alternative or novel methodologies, e.g., machine learning, artificial intelligence, novel simulation methods, and intelligence gathering. The model parameters that commonly appear in game-theoretic analyses may be estimated by applying empirical data, which can be continuously improved through compilation by statistics bureaus and other actors.

Future research should generate results that are less dependent on specific assumptions, to ensure robust results that are valid across a variety of different circumstances, applicable for policymakers and decision-makers. One challenge in this regard is the balance to be struck between generalizability, simplicity, and precision, where, usually, only two of these criteria can simultaneously be satisfied.

Future research should broaden the cyber focus within traffic and transportation, accounting for air, land, and sea and distinguishing between the transport of humans and goods, etc. Such research should be extended to the transport of information and communication, which increasingly occurs wirelessly. This opens up new attack vectors. Cyber security within centralized and decentralized blockchain technology should also be researched. The 19 July 2024 CrowdStrike Information Technology outage highlights the need to analyze how individuals, firms, governments, and others depend on software and hardware from various contributors and potentially interceptors, which may have benign or less benign objectives and may possess unknown competences in rapidly changing environments.

Whereas this review has focused on traffic and transportation and cyber security education and board games, cyber security will, in the future, play an increasing role also in other domains, such as finance, banking, insurance, healthcare, emergency services, energy, utilities, water and power supplies, telecommunications, governments, public

sector agencies, military, aviation, supply chains, logistics, manufacturing, education, retail, e-commerce, media, entertainment, smart cities, and critical infrastructure. Examples of its roles are fraud detection and prevention, regulatory compliance, security related to property rights, data storage, privacy, transparency, transactions, network operations, cloud operation, and software/hardware updates.

Several research gaps exist from a game-theoretic perspective in the cyber security literature, which are promising for future research.

1. Multiple objectives: Utility functions should be developed focusing on the worst- and best-case scenarios, minimizing the costs, maximizing the benefits or security, weighing human vs. economic vs. symbolic value, and weighing multiple objectives against each other.
2. Incomplete information: Games should account for players being uncertain about their surroundings and the future, including other players' preferences and beliefs.
3. Mixed strategies: Games should focus on players choosing strategies probabilistically.
4. Stochastic games: Randomness should be incorporated into the players' strategies and their surroundings.
5. The time dimension: Repeated and dynamic games should be developed accounting for new events and information, where adversaries react to each other in various sequences.
6. Complexity: Models should account for increasingly complex cyber security challenges, develop more efficient solution methods, utilize increasingly available supercomputers to solve large-scale problems, and question the available strategies, utility combinations, and the games that players play.
7. Empirical support: The models should be tested experimentally and in real-life settings to ensure their realism, validation, and practical implementation.
8. Behavioral game theory: Theory and empirics should be combined to ensure the increased realism of economic, political, and social interactions, accounting for bounded rationality and risk attitudes.
9. Learning: How players learn in a novel field such as cyber security should be analyzed, accounting for the adaptation, reinforcement, and adjustment of strategies, preferences, and beliefs.
10. Cooperative games: How players form coalitions to share costs and benefits and obtain cyber security should be scrutinized.
11. Interdisciplinarity: Game theory should be combined with other disciplines within the technological, natural, social, and human sciences to obtain more holistic insights. Examples of disciplines include Internet of Things security, 5G and next-generation network security, artificial intelligence, machine learning, quantum computing, cryptography, blockchain and distributed ledger technology, zero-trust architectures, privacy-enhancing technologies, cyber–physical systems, user education and awareness, psychological profiling, advanced threat intelligence, and frameworks for regulation, compliance, adaptation, resilience, and recovery.

12. Conclusions

This article reviews attacker–defender games, which have a longer and broader history than the more recent and narrower phenomenon of cyber security, which inevitably involves attack and defense. Hence, this review starts with a strong focus on attack and defense models, multiple targets, multiple attackers and defenders, multiple periods, and various characteristics of defense and attack. The literature commonly considers one player defending or attacking one component in a system, multiple-attacker and/or multiple-defender games, and multiple-period attacker–defender games. Defense and attack games have various characteristics. For example, they may involve security screening and inspection, the detection of invaders, and jamming.

Whereas the majority of attacker–defender games in the literature assumes complete information, as a transition to cyber security, the prominent role of incomplete information

is reviewed, involving multiple targets, secrecy and deception, threat propagation, and trust and reputation. Information about the players' characteristics may be drawn probabilistically. Thereafter, information sharing is considered, followed by cyber stockpiling, deterrence, and resilience. The joint operation of information sharing and security investment is reviewed. Players may prefer to receive information from others but not provide information, which suggests a free-rider dilemma, unless a social planner is introduced. Firms may experience cyber attacks or breaches directly or indirectly through shared network ties or dependencies through supply chains. Firms may tend to underinvest in security and free-ride unless otherwise incentivized. Cyber attackers may produce cyber munitions for present use or stockpile zero-day cyber vulnerabilities for future use. Cyber security deterrence and resilience are considered.

The presence of incomplete information in cyber security makes a review of stochastic analyses relevant, acknowledging the many uncertainties and probabilities of states, strategies, and outcomes that are involved. Most of these consider one defender and one attacker. They cover a variety of phenomena, including intrusion detection, jamming, and eavesdropping.

The review concludes with two topics having attracted substantial attention in recent years. One is cyber security in traffic and transportation, partly influenced by the communication of GPS data between moving units such as self-driving cars. The second is cyber security education and board games, tabletop games, card games, and experimental games, to enable people to face cyber threats in real life. Such games also involve learning, training, and awareness and are influenced by the ubiquitous presence and risk of portable electronic devices in human life. Strengths, weaknesses, opportunities, and future research are considered.

Funding: J. Zhuang's effort was partially supported by the U.S. Department of Homeland Security under Grant Award Numbers 24STADA00002 and 22STESE00001-03-04. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: Author Jonathan W. Welburn is employed by Pardee RAND Graduate School. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A. Players and Phenomena in the Reviewed Articles

Table A1. Players and phenomena in the reviewed articles.

	Reference	Players	Phenomena
1	Acemoglu, Malekian and Ozdaglar [81]	Multiple agents, one attacker	Network security investment against contagious infection
2	Ackerman, Zhuang and Weerasuriya [14]	Extremist groups, Western societies	Terrorist collaboration
3	Alpcan and Basar [80]	One defender, one attacker	Stochastic network intrusion detection
4	Amin and Johansson [1]	Multiple players	Review: Cyber security
5	Backhaus, Bent, Bono, Lee, Tracey, Wolpert, Xie and Yildiz [98]	One defender, one attacker	Defense against a cyber–physical intruder with attack-resilient smart grids
6	Baliga, De Mesquita and Wolitzky [95]	Multiple attackers, one victim	Victim is uncertain about attributing an attack to an attacker
7	Bandyopadhyay, Jacob and Raghunathan [75]	Two firms	Tightly integrated communication networks and supply chains increase security investment

Table A1. *Cont.*

	Reference	Players	Phenomena
8	Banks, Gallego, Naveiro and Ríos Insua [51]	One defender, one attacker	Adversarial risk analysis: An overview
9	Bier [52]	One defender, one attacker	Attacker with unknown preferences attacking one of many targets
10	Bier, Oliveros and Samuelson [53]	One defender, one attacker	Attacker with unknown preferences attacking one of many targets
11	Brown, Kline, Thomas, Washburn and Wood [33]	One defender, one attacker	Applying ships, aircraft, etc., to defend against submarine attacks.
12	Brown, Carlyle, Harney, Skroch and Wood [31]	One defender, one attacker	Max–min analysis of critical path to interdict nuclear-weapons project
13	Clarke and Knake [92]	Multiple players	Cyber war
14	Cone, Irvine, Thompson and Nguyen [119]	Multiple players	Interactive video game to build cyber security awareness
15	Crosston [90]	Multiple players	Mutually assured debilitation to ensure cyber deterrence
16	Dighe, Zhuang and Bier [43]	Two defenders, one attacker	Attack deterrence through secretive centralized or decentralized defense
17	Do, Tran, Hong, Kamhoua, Kwiat, Blasch, Ren, Pissinou and Iyengar [2]	Multiple players	Review: Cyber security
18	Dong, Chen, Hunt and Zhuang [47]	One defender, one attacker	Forecast information and risk control in defensive resource allocation
19	Dresher [87]	Multiple players	Games of strategy
20	Edwards, Furnas, Forrest and Axelrod [94]	One attacker, one victim	Victim is uncertain about attributing an attack to an attacker
21	Etesami and Basar [3]	Multiple players	Review: Cyber–physical systems
22	Frey, Rashid, Anthonysamy, Pinto-Albuquerque and Naqvi [120]	Multiple players	Tabletop game to experiment with security risks
23	Futter [121]	Multiple players	War games for cyberthreats, nuclear security, and arms control
24	Gal-Or and Ghose [66]	Two firms, one social planner	Information sharing and security investment as strategic complements
25	Gao and Shi [102]	One defender, one attacker	Defender–attacker–defender game for cyber–physical power systems
26	Garnaev, Baykal-Gursoy and Poor [38]	One defender, one attacker	Stochastic communication subject to jamming and eavesdropping
27	Gerald, Matthew, Ahmad and Jeffrey [32]	One defender, one attacker	Port radar surveillance of speedboats
28	Gordon, Loeb and Lucyshyn [65]	Two firms	Information sharing, security investment, free-riding
29	Guikema and Aven [4]	Multiple players	Review: Risk from various perspectives
30	Gupta, Langbort and Basar [61]	One defender, one attacker	Asymmetric information in a cyber–physical system
31	Han and Choi [64]	One defender, one attacker	Attacker mimics a normal user in a cyber system
32	Han and Choi [62]	One defender, one attacker	Penalizing a defender for false alarms in a cyber security intrusion detection system
33	Haphuriwat, Bier and Willis [30]	One defender, one attacker	Inspection, deterrence, and retaliation in smuggling
34	Harta, Margheri, Paci and Sassonea [122]	Multiple players	Cyber security awareness and education tabletop game
35	Hausken [13]	Multiple players	Probabilistic risk analysis, different system configurations
36	Hausken [67]	Two firms, one attacker, one social planner	Information sharing and security investment as strategic substitutes

Table A1. *Cont.*

	Reference	Players	Phenomena
37	Hausken [54]	One defender, one attacker	Attacker's resources and target valuations are probabilistic
38	Hausken [68]	Two hackers, one firm	Information sharing, attack, free-riding, complements, substitutes
39	Hausken [69]	Two hackers, one firm	Information sharing, four-period game, deterrence
40	Hausken [70]	Two hackers, two firms	Information sharing, four-period game, deterrence
41	Hausken [135]	One defender, one attacker	Special versus general protection and attack of parallel and series components
42	Hausken [71]	Two hackers, one firm	Information sharing, proactive and retroactive defense, four-period game
43	Hausken [5]	Multiple players	Review: Cyber resilience
44	Hausken [6]	Multiple players	Review: Attack and defense for various systems
45	Hausken and Levitin [7]	Multiple players	Review: Defense and attack in reliability systems
46	Hausken and Welburn [84]	Two players	Zero-day attacks with stockpiling
47	Hausken and Zhuang [22]	One defender, one attacker	Stockpiling terrorist
48	Hausken and Zhuang [21]	One defender, one attacker	Stockpiling terrorist
49	Hausken and Zhuang [19]	One defender, one attacker	T periods, random resource determination
50	Hausken and Zhuang [23]	One defender, one attacker	Terrorist chooses when to attack and can be deterred
51	He and Zhuang [56]	One government, one terrorist	Contracts or mutually beneficial arrangements to deter attacks
52	He, Devine and Zhuang [72]	Decision-theoretic	Information sharing, public–private partnership, cost–benefit analysis
53	Hu, Liu, Chen, Zhang and Liu [104]	One defender, one attacker	Stochastic evolution of cyber security
54	Huang, Zhou, Qin and Tu [105]	One defender, one attacker	Stochastic analysis of cyber–physical system
55	Hunt, Agarwal and Zhuang [59]	One defender, one attacker	Technology adoption and disclosure of secrecy in airport security
56	Hunt and Zhuang [8]	Multiple players	Review: Attack and defense within different systems
57	Huo, Dong, Qian and Jing [114]	Multiple players	Vehicular cyber–physical coalition formation game
58	Jasper [93]	Multiple players	Deterring malicious behavior in cyberspace
59	Jensen [91]	Multiple players	Cyber deterrence
60	Jin, Zhang, Hu, Zhang and Sun [123]	One defender, one attacker	Reinforcement learning denial of service analysis in cyber–physical system
61	Jose and Zhuang [20]	One defender, one attacker	Technology adoption and accumulation in multiple periods
62	Kanellopoulos and Vamvoudakis [124]	Multiple players	Cyber–physical dynamic security training game, bounded rationality, level-k intelligence
63	Kolokoltsov and Bensoussan [106]	Multiple defenders, one hacker	Mean-field stochastic analysis of cyber security
64	Kott, Swami and McDaniel [9]	Multiple players	Review: Cyber game changers
65	Kovenock and Roberson [82]	One defender, one attacker	Multiple networks with intra-network strategic complementarities among targets

Table A1. *Cont.*

	Reference	Players	Phenomena
66	Levitin, Hausken, Taboada and Coit [73]	One defender, one attacker	Information storage in multiple blocks with maximum number of copies of each block
67	Li, Chen, Huang, Yao, Xia and Mei [103]	Multiple players	Evolutionary competition between virus propagation to protect cyber nodes within power systems
68	Li and Xu [79]	One retailer, multiple suppliers	Joint decision-making, security risk compensation, information sharing, free-riding
69	Libicki [88]	Multiple players	Cyber deterrence and cyber war
70	Liu, Zhang, Zhu, Tan and Yin [60]	One defender, one attacker	Threat propagation between nodes in cyber–physical systems with incomplete information
71	Maqbool, Aggarwal, Pammi and Dutt [125]	Multiple defenders, multiple hackers	Laboratory experimental game involving cyber attacks
72	Miao and Li [107]	Multiple defenders, multiple attackers	Susceptible–infected–removed epidemic mean-field stochastic cyber security analysis
73	Miao, Zhu, Pajic and Pappas [108]	One defender, one attacker	Zero-sum stochastic finite horizon analysis of cyber–physical system
74	Miao, Wang, Li, Xu and Zhou [109]	Multiple defenders, multiple attackers	Mean-field cyber security analysis with discrete-time dynamics
75	Nagurney, Nagurney and Shukla [76]	Retailers and consumers	Increased supply chain interdependence can increase vulnerabilities to attack
76	Nagurney and Shukla [77]	Multiple firms	Information sharing causes financial and security benefits
77	Nicho [126]	Multiple players	Education game to build cyber security awareness
78	Nicholas and Alderson [35]	One defender, one attacker	Operating a wireless network attacked with jamming
79	Nikoofal and Zhuang [39]	One defender, one attacker	Disclosure versus secrecy of a defense system
80	Njilla, Pissinou and Makki [63]	One provider, one attacker, one user	Breaching a service provider's database to expose a user's private information
81	Nye [89]	Multiple players	Nuclear lessons for cyber security
82	O'Connor, Hasshu, Bielby, Colreavy-Donnelly, Kuhn, Caraffini and Smith [127]	Multiple players	Training game for cyber security
83	Orojloo and Azgomi [34]	One defender, one attacker	Intrusion and disruption of a cyber–physical system
84	Orojloo and Azgomi [110]	One defender, one attacker	Stochastic intrusion and disruption of a cyber–physical system
85	Pala and Zhuang [29]	One defender, one attacker, one group of applicants	Impatient applicants, Markov process
86	Pala and Zhuang [10]	Multiple players	Review: Information sharing, considerations of stakeholders including firms, governments, citizens, and adversaries
87	Ravishankar, Rao and Kumar [128]	Multiple defenders, multiple attackers	Software cyber warfare testbed game for critical infrastructure
88	Rios Insua, Rios and Banks [49]	One defender, one attacker	Adversarial risk analysis
89	Rios Insua, Rios and Banks [48]	One defender, one attacker	Adversarial risk analysis, level-k thinking
90	Rothschild, McLay and Guikema [50]	One defender, one attacker	Adversarial risk analysis with incomplete information, level-k approach
91	Roy, Ellis, Shiva, Dasgupta, Shandilya and Wu [11]	Multiple players	Review: Cyber security

Table A1. *Cont.*

	Reference	Players	Phenomena
92	Sanjab, Saad and Basar [115]	One defender, one attacker	Benign or malicious interdictor targeting unmanned aerial vehicle operator
93	Schelling [86]	Multiple players	Strategy of conflict
94	Schramm, Alderson, Carlyle and Dimitrov [85]	Two players	Zero-day attacks
95	Sedjelmaci, Brahmi, Ansari and Rehmani [116]	Multiple players	Hierarchical vehicular network game to protect against cyber attacks
96	Sedjelmaci, Hadji and Ansari [12]	Multiple players	Review: Cyber security defense of intelligent transportation systems
97	Shah and Agarwal [129]	Multiple players	Smartphone security awareness card game
98	Shan and Zhuang [24]	One defender, one attacker	Retaliation for smuggling may occur in the third period
99	Shan and Zhuang [18]	Two defenders, two attackers	Disruption of terrorism supply chain assuming subsidization and proliferation
100	Shen and Feng [101]	Multiple players	Stackelberg interaction between interdependent non-malicious cyber–physical systems
101	Shukla, An, Chakrabortty and Duel-Hallen [100]	One defender, one attacker	Stackelberg defense of networked control system of nodes
102	Simon [134]	Multiple players	Near decomposability of players
103	Simon and Omar [78]	Multiple defenders, one attacker	Security investment is suboptimal without coordination
104	Singh, Borkotokey, Lahcen and Mohapatra [111]	One defender, one attacker	Stochastic cyber security with incomplete information and bounded rationality
105	Song and Zhuang [27]	One defender, one attacker, one group of applicants	N periods, security screening problem with screening errors
106	Song and Zhuang [26]	One defender, one attacker, one group of applicants	Two periods, security screening problem with screening errors
107	Song and Zhuang [28]	One defender, one attacker, one group of applicants	Parallel-queue security screening problem with incomplete information
108	Tosh, Sengupta, Kamhoua and Kwiat [74]	Multiple firms	Information sharing, dynamic cost adaptation, learning heuristic, evolution
109	Tseng, Yang, Shih and Shan [130]	Multiple players	Cyber security education board game
110	Wang and Bier [44]	One defender, one attacker	Multitarget resource allocation with incomplete information and multi-attribute utility
111	Wang and Bier [45]	One defender, one attacker	Stackelberg multitarget resource allocation while quantifying adversary capabilities
112	Wang, Welburn and Hausken [83]	Two players	Zero-day attacks with stockpiling
113	Wang and Zhuang [25]	One defender, one attacker, one group of applicants	Congestion, security, incomplete information
114	Welburn, Grana and Schwindt [96]	One attacker, one victim	Victim has private information and is uncertain about attributing an attack to an attacker
115	Wu, Dong and Wang [117]	One defender, one attacker	Air traffic management of cyber–physical system with incomplete information
116	Xing, Zhao, Basar and Xia [112]	Multiple sensors	Resource-constrained security investment in cyber–physical network with asymmetric information
117	Xu, Wu and Tao [36]	One defender, one attacker	Mobile communication subject to jamming and eavesdropping
118	Xu and Zhuang [15]	One defender, one attacker	Costly learning and counter-learning with private defender information
119	Xu and Baykal-Gursoy [37]	One defender, one attacker	Wireless communication subject to jamming and eavesdropping

Table A1. *Cont.*

	Reference	Players	Phenomena
120	Xu and Zhuang [15]	One defender, multiple attackers	Defender moves first, attackers move sequentially thereafter
121	Yamin, Katt and Nowostawski [131]	Multiple players	Training game to learn about cyber security
122	Yang, Xiang, Liao and Yang [118]	One defender, one attacker	Coupled vehicular transportation network and cyber–physical power system
123	Yasin, Liu, Li, Wang and Zowghi [132]	Multiple players	Education game to learn about cyber security
124	Yolmeh and Baykal-Gürsoy [55]	One defender, one attacker	Unknown distribution of information about target values and detection probabilities
125	Zeijlemaker, Rouwette, Cunico, Armenia and von Kutzschenbach [133]	Multiple players	Cyber security board game to train bank managers
126	Zhai, Peng and Zhuang [46]	One defender, one attacker	Defender's utility is survivability, attacker's utility is expected number of destroyed elements
127	Zhang and Liu [113]	One defender, one attacker	Stochastic analysis of cyber security, bounded rationality, learning
128	Zhang and Malacaria [99]	One defender, one attacker	Mixed-integer cyber security controls against multi-stage attacks
129	Zhu and Basar [97]	One defender, one attacker	Robustness, security, and resilience of cyber–physical control systems
130	Zhuang [17]	Multiple players	Security investment among interdependent agents receiving subsidies
131	Zhuang and Bier [58]	One defender, one attacker	Balancing terrorism and natural disasters
132	Zhuang and Bier [41]	Multiple players	Reasons for secrecy and deception in resource allocation
133	Zhuang and Bier [40]	One defender, one attacker	Truthful disclosure, secrecy, or deception in anti-terrorism
134	Zhuang, Bier and Alagoz [42]	Multiple defenders	Interdependent security with time discounting
135	Zhuang, Bier and Gupta [16]	Multiple defenders	Interdependent security with time discounting

References

1. Amin, S.; Johansson, K.H. Preface to the Focused Issue on Dynamic Games in Cyber Security. *Dyn. Games Appl.* **2019**, *9*, 881–883. [CrossRef]
2. Do, C.T.; Tran, N.H.; Hong, C.; Kamhoua, C.A.; Kwiat, K.A.; Blasch, E.; Ren, S.; Pissinou, N.; Iyengar, S.S. Game theory for cyber security and privacy. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 30. [CrossRef]
3. Etesami, S.R.; Basar, T. Dynamic Games in Cyber-Physical Security: An Overview. *Dyn. Games Appl.* **2019**, *9*, 884–913. [CrossRef]
4. Guikema, S.; Aven, T. Assessing Risk from Intelligent Attacks: A Perspective on Approaches. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 478–483. [CrossRef]
5. Hausken, K. Cyber resilience in firms, organizations and societies. *Internet Things* **2020**, *11*, 100204. [CrossRef]
6. Hausken, K. Fifty Years of Operations Research in Defense. *Eur. J. Oper. Res.* **2024**, *318*, 355–368. [CrossRef]
7. Hausken, K.; Levitin, G. Review of Systems Defense and Attack Models. *Int. J. Perform. Eng.* **2012**, *8*, 355–366. [CrossRef]
8. Hunt, K.; Zhuang, J. A review of attacker-defender games: Current state and paths forward. *Eur. J. Oper. Res.* **2024**, *313*, 401–417. [CrossRef]
9. Kott, A.; Swami, A.; McDaniel, P. Security Outlook: Six Cyber Game Changers for the Next 15 Years. *Computer* **2014**, *47*, 104–106. [CrossRef]
10. Pala, A.; Zhuang, J. Information Sharing in Cybersecurity: A Review. *Decis. Anal.* **2019**, *16*, 172–196. [CrossRef]
11. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the System Sciences (HICSS), 2010 43rd Hawaii International Conference, Honolulu, HI, USA, 5–8 January 2010; pp. 1–10.
12. Sedjelmaci, H.; Hadji, M.; Ansari, N. Cyber Security Game for Intelligent Transportation Systems. *IEEE Netw.* **2019**, *33*, 216–222. [CrossRef]

13. Hausken, K. Probabilistic Risk Analysis and Game Theory. *Risk Anal.* **2002**, *22*, 17–27. [CrossRef] [PubMed]
14. Ackerman, G.; Zhuang, J.; Weerasuriya, S. Cross-Milieu Terrorist Collaboration: Using Game Theory to Assess the Risk of a Novel Threat. *Risk Anal.* **2017**, *37*, 342–371. [CrossRef] [PubMed]
15. Xu, Z.; Zhuang, J. A Study on A Sequential One-Defender-N-Attacker Game. *Risk Anal.* **2019**, *39*, 1414–1432. [CrossRef] [PubMed]
16. Zhuang, J.; Bier, V.M.; Gupta, A. Subsidies in Interdependent Security with Heterogeneous Discount Rates. *Eng. Econ.* **2007**, *52*, 1–19. [CrossRef]
17. Zhuang, J. Impacts of Subsidized Security on Stability and Total Social Costs of Equilibrium Solutions in an N-Player Game with Errors. *Eng. Econ.* **2010**, *55*, 131–149. [CrossRef]
18. Shan, X.; Zhuang, J. Subsidizing to Disrupt a Terrorism Supply Chain—A Four-Player Game. *J. Oper. Res. Soc.* **2014**, *65*, 1108–1119. [CrossRef]
19. Hausken, K.; Zhuang, J. Governments' and Terrorists' Defense and Attack in a T-Period Game. *Decis. Anal.* **2011**, *8*, 46–70. [CrossRef]
20. Jose, V.R.R.; Zhuang, J. Technology Adoption, Accumulation, and Competition in Multi-period Attacker-Defender Games. *Mil. Oper. Res.* **2013**, *18*, 33–47. [CrossRef]
21. Hausken, K.; Zhuang, J. Defending against a Terrorist Who Accumulates Resources. *Mil. Oper. Res.* **2011**, *16*, 21–39. [CrossRef]
22. Hausken, K.; Zhuang, J. Defending against a Stockpiling Terrorist. *Eng. Econ.* **2011**, *56*, 321–353.
23. Hausken, K.; Zhuang, J. The Timing and Deterrence of Terrorist Attacks due to Exogenous Dynamics. *J. Oper. Res. Soc.* **2012**, *63*, 726–735. [CrossRef]
24. Shan, X.; Zhuang, J. Modeling Credible Retaliation Threats in Deterring the Smuggling of Nuclear Weapons Using Partial Inspection-A Three-Stage Game. *Decis. Anal.* **2014**, *11*, 43–62. [CrossRef]
25. Wang, X.; Zhuang, J. Balancing Congestion and Security in the Presence of Strategic Applicants with Private Information. *Eur. J. Oper. Res.* **2011**, *212*, 100–111. [CrossRef]
26. Song, C.; Zhuang, J. Two-Stage Security Screening Strategies in the Face of Strategic Applicants, Congestions and Screening Errors. *Ann. Oper. Res.* **2017**, *258*, 237262. [CrossRef]
27. Song, C.; Zhuang, J. N-Stage Security Screening Strategies in the Face of Strategic Applicants. *Reliab. Eng. Syst. Saf.* **2017**, *165*, 292–301. [CrossRef]
28. Song, C.; Zhuang, J. Modelling Precheck Parallel Screening Process in the Face of Strategic Applicants with Incomplete Information and Screening Errors. *Risk Anal.* **2018**, *38*, 118–133. [CrossRef]
29. Pala, A.; Zhuang, J. Security Screening Queues with Impatient Applicants: A New Model with a Case Study. *Eur. J. Oper. Res.* **2018**, *265*, 919–930. [CrossRef]
30. Haphuriwat, N.; Bier, V.M.; Willis, H.H. Deterring the Smuggling of Nuclear Weapons in Container Freight through Detection and Retaliation. *Decis. Anal.* **2011**, *8*, 88–102. [CrossRef]
31. Brown, G.G.; Carlyle, W.M.; Harney, R.C.; Skroch, E.M.; Wood, R.K. Interdicting a Nuclear-Weapons Project. *Oper. Res.* **2009**, *57*, 866–877. [CrossRef]
32. Gerald, G.B.; Matthew, C.; Ahmad, A.-G.; Jeffrey, K. A defender-attacker optimization of Port Radar surveillance: Defender-Attacker Optimization of Port Surveillance. *Nav. Res. Logist.* **2011**, *58*, 223–235. [CrossRef]
33. Brown, G.; Kline, J.; Thomas, A.; Washburn, A.; Wood, R.K. A Game-Theoretic Model for Defense of an Oceanic Bastion against Submarines. *Mil. Oper. Res.* **2011**, *16*, 25–40. [CrossRef]
34. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [CrossRef]
35. Nicholas, P.J.; Alderson, D.L. Fast Design of Wireless Mesh Networks to Defend against Worst-Case Jamming. *Mil. Oper. Res.* **2018**, *23*, 5–20.
36. Xu, J.; Wu, H.C.; Tao, X.F. 5G Cyberspace Security Game. *J. Electron. Inf. Technol.* **2020**, *42*, 2319–2329. [CrossRef]
37. Xu, Z.; Baykal-Gursoy, M. Power Allocation for Cooperative Jamming against a Strategic Eavesdropper Over Parallel Channels. *IEEE Trans. Inf. Forensic Secur.* **2023**, *18*, 846–858. [CrossRef]
38. Garnaev, A.; Baykal-Gursoy, M.; Poor, H.V. A Game Theoretic Analysis of Secret and Reliable Communication with Active and Passive Adversarial Modes. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2155–2163. [CrossRef]
39. Nikoofal, M.E.; Zhuang, J. On the Value of Exposure and Secrecy of Defense System: First-Mover Advantage Vs. Robustness. *Eur. J. Oper. Res.* **2015**, *246*, 320–330. [CrossRef]
40. Zhuang, J.; Bier, V.M. Secrecy and Deception at Equilibrium, with Applications to Anti-Terrorism Resource Allocation. *Def. Peace Econ.* **2011**, *22*, 43–61. [CrossRef]
41. Zhuang, J.; Bier, V.M. Reasons for Secrecy and Deception in Homeland-Security Resource Allocation. *Risk Anal.* **2010**, *30*, 1737–1743. [CrossRef]
42. Zhuang, J.; Bier, V.M.; Alagoz, O. Modeling Secrecy and Deception in a Multiple-Period Attacker-Defender Signaling Game. *Eur. J. Oper. Res.* **2010**, *203*, 409–418. [CrossRef]
43. Dighe, N.S.; Zhuang, J.; Bier, V.M. Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-Effective Attacker Deterrence. *Int. J. Perform. Eng.* **2009**, *5*, 31–43.
44. Wang, C.; Bier, V.M. Target-Hardening Decisions Based on Uncertain Multiattribute Terrorist Utility. *Decis. Anal.* **2011**, *8*, 286–302. [CrossRef]

45. Wang, C.; Bier, V.M. Quantifying Adversary Capabilities to Inform Defensive Resource Allocation. *Risk Anal.* **2016**, *36*, 756–775. [CrossRef]
46. Zhai, Q.; Peng, R.; Zhuang, J. Defender-Attacker Games with Asymmetric Player Utilities. *Risk Anal.* **2020**, *40*, 408–420. [CrossRef] [PubMed]
47. Dong, Y.; Chen, X.; Hunt, K.; Zhuang, J. Defensive Resource Allocation: The Roles of Forecast Information and Risk Control. *Risk Anal.* **2021**, *41*, 1304–1322. [CrossRef]
48. Rios Insua, D.; Rios, J.; Banks, D. Modeling Opponents in Adversarial Risk Analysis. *Risk Anal.* **2016**, *36*, 742–755. [CrossRef]
49. Rios Insua, D.; Rios, J.; Banks, D. Adversarial Risk Analysis. *J. Am. Stat. Assoc.* **2009**, *104*, 841–854. [CrossRef]
50. Rothschild, C.; McLay, L.; Guikema, S. Adversarial Risk Analysis with Incomplete Information: A Level-k Approach. *Risk Anal.* **2012**, *32*, 1219–1231. [CrossRef] [PubMed]
51. Banks, D.; Gallego, V.; Naveiro, R.; Ríos Insua, D. Adversarial risk analysis: An overview. *Wiley Interdiscip. Rev. Comput. Stat.* **2022**, *14*, e1530. [CrossRef]
52. Bier, V.M. Choosing What to Protect. *Risk Anal.* **2007**, *27*, 607–620. [CrossRef]
53. Bier, V.M.; Oliveros, S.; Samuelson, L. Choosing what to protect: Strategic defensive allocation against an unknown attacker. *J. Public Econ. Theory* **2007**, *9*, 563–587. [CrossRef]
54. Hausken, K. Choosing What to Protect When Attacker Resources and Asset Valuations are Uncertain. *Oper. Res. Decis.* **2014**, *24*, 23–44.
55. Yolmeh, A.; Baykal-Gürsoy, M. A robust approach to infrastructure security games. *Comput. Ind. Eng.* **2017**, *110*, 515–526. [CrossRef]
56. He, F.; Zhuang, J. Modelling 'Contracts' between a Terrorist Group and a Government in a Sequential Game. *J. Oper. Res. Soc.* **2012**, *63*, 790–809. [CrossRef]
57. Xu, J.; Zhuang, J. Modeling Costly Learning and Counter-learning in a Defender-attacker Game with Private Defender Information. *Ann. Oper. Res.* **2016**, *236*, 271–289. [CrossRef]
58. Zhuang, J.; Bier, V.M. Balancing Terrorism and Natural Disasters: Defensive Strategy with Endogenous Attacker Effort. *Oper. Res.* **2007**, *55*, 976–991. [CrossRef]
59. Hunt, K.; Agarwal, P.; Zhuang, J. Technology Adoption for Airport Security: Modeling Public Disclosure and Secrecy in an Attacker-defender Game. *Reliab. Eng. Syst. Saf.* **2021**, *207*, 107355. [CrossRef]
60. Liu, X.X.; Zhang, J.X.; Zhu, P.D.; Tan, Q.P.; Yin, W. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Comput. Secur.* **2021**, *102*, 102138. [CrossRef]
61. Gupta, A.; Langbort, C.; Basar, T. Dynamic Games with Asymmetric Information and Resource Constrained Players with Applications to Security of Cyberphysical Systems. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 71–81. [CrossRef]
62. Han, K.; Choi, J.H. Implications of false alarms in dynamic games on cyber-security. *Chaos Solitons Fractals* **2023**, *169*, 113322. [CrossRef]
63. Njilla, L.Y.; Pissinou, N.; Makki, K. Game theoretic modeling of security and trust relationship in cyberspace. *Int. J. Commun. Syst.* **2016**, *29*, 1500–1512. [CrossRef]
64. Han, K.; Choi, J.H. A Reputation Game on Cyber-Security and Cyber-Risk Calibration. *Appl. Math. Optim.* **2022**, *85*, 13. [CrossRef]
65. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. [CrossRef]
66. Gal-Or, E.; Ghose, A. The Economic Incentives for Sharing Security Information. *Inf. Syst. Res.* **2005**, *16*, 186–208. [CrossRef]
67. Hausken, K. Information Sharing Among Firms and Cyber Attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. [CrossRef]
68. Hausken, K. A Strategic Analysis of Information Sharing Among Cyber Attackers. *J. Inf. Syst. Technol. Manag.* **2015**, *12*, 245–270. [CrossRef]
69. Hausken, K. Information Sharing Among Cyber Hackers in Successive Attacks. *Int. Game Theory Rev.* **2017**, *19*, 33. [CrossRef]
70. Hausken, K. Security Investment, Hacking, and Information Sharing between Firms and between Hackers. *Games* **2017**, *8*, 23. [CrossRef]
71. Hausken, K. Proactivity and Retroactivity of Firms and Information Sharing of Hackers. *Int. Game Theory Rev.* **2018**, *20*, 1750027. [CrossRef]
72. He, M.; Devine, L.; Zhuang, J. Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders using a Decision Theoretic Approach. *Risk Anal.* **2018**, *38*, 215–225. [CrossRef] [PubMed]
73. Levitin, G.; Hausken, K.; Taboada, H.A.; Coit, D.W. Data Survivability Vs. Security in Information Systems. *Reliab. Eng. Syst. Saf.* **2012**, *100*, 19–27. [CrossRef]
74. Tosh, D.; Sengupta, S.; Kamhoua, C.A.; Kwiat, K.A. Establishing evolutionary game models for CYBer security information EXchange (CYBEX). *J. Comput. Syst. Sci.* **2018**, *98*, 27–52. [CrossRef]
75. Bandyopadhyay, T.; Jacob, V.; Raghunathan, S. Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest. *Inf. Technol. Manag.* **2010**, *11*, 7–23. [CrossRef]
76. Nagurney, A.; Nagurney, L.S.; Shukla, S. A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability. In *Computation, Cryptography, and Network Security*; Daras, N.J., Rassias, M.T., Eds.; Springer International Publishing: Cham, Swizerland, 2015; pp. 381–398.

77. Nagurney, A.; Shukla, S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *Eur. J. Oper. Res.* **2017**, *260*, 588–600. [CrossRef]
78. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* **2020**, *282*, 161–171. [CrossRef]
79. Li, Y.; Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *Int. J. Prod. Res.* **2020**, *59*, 1216–1238. [CrossRef]
80. Alpcan, T.; Basar, T. An intrusion detection game with limited observations. In Proceedings of the 12th International Symposium on Dynamic Games and Applications, Sophia Antipolis, France, 3–6 July 2006.
81. Acemoglu, D.; Malekian, A.; Ozdaglar, A. Network security and contagion. *J. Econ. Theory* **2016**, *166*, 536–585. [CrossRef]
82. Kovenock, D.; Roberson, B. The Optimal Defense of Networks of Targets. *Econ. Inq.* **2018**, *56*, 2195–2211. [CrossRef]
83. Wang, G.; Welburn, J.W.; Hausken, K. A Two-Period Game Theoretic Model of Zero-Day Attacks with Stockpiling. *Games* **2020**, *11*, 64. [CrossRef]
84. Hausken, K.; Welburn, J.W. Attack and Defense Strategies in Cyber War Involving Production and Stockpiling of Zero-Day Cyber Exploits. *Inf. Syst. Front.* **2021**, *23*, 1609–1620. [CrossRef]
85. Schramm, H.; Alderson, D.L.; Carlyle, W.M.; Dimitrov, N.B. *A Game Theoretic Model of Strategic Conflict in Cyberspace*; Naval Postgraduate School: Monterey, CA, USA, 2012.
86. Schelling, T.C. *The Strategy of Conflict*; Harvard University Press: Cambridge, MA, USA, 1960.
87. Dresher, M. *Games of Strategy: Theory and Applications*; RAND Corporation: Santa Monica, CA, USA, 1961.
88. Libicki, M.C. *Cyberdeterrence and Cyberwar*; Rand Corporation: Santa Monica, CA, USA, 2009.
89. Nye, J.S. Nuclear lessons for cyber security? *Strateg. Stud. Q.* **2011**, *5*, 18–38.
90. Crosston, M.D. World gone cyber MAD: How "Mutually Assured Debilitation" is the best hope for cyber deterrence. *Strateg. Stud. Q.* **2011**, *5*, 100–116.
91. Jensen, E.T. Cyber deterrence. *Emory Int'l L. Rev.* **2012**, *26*, 773. [CrossRef]
92. Clarke, R.A.; Knake, R.K. *Cyber War*; Tantor Media, Incorporated: Old Saybrook, CT, USA, 2014.
93. Jasper, S. Deterring malicious behavior in cyberspace. *Strateg. Stud. Q.* **2015**, *9*, 60–85.
94. Edwards, B.; Furnas, A.; Forrest, S.; Axelrod, R. Strategic aspects of cyberattack, attribution, and blame. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 2825–2830. [CrossRef]
95. Baliga, S.; De Mesquita, E.B.; Wolitzky, A. Deterrence with Imperfect Attribution. *Am. Political Sci. Rev.* **2020**, *114*, 1155–1178. [CrossRef]
96. Welburn, J.; Grana, J.; Schwindt, K. Cyber deterrence with imperfect attribution and unverifiable signaling. *Eur. J. Oper. Res.* **2023**, *306*, 1399–1416. [CrossRef]
97. Zhu, Q.Y.; Basar, T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Syst. Mag.* **2015**, *35*, 46–65. [CrossRef]
98. Backhaus, S.; Bent, R.; Bono, J.; Lee, R.; Tracey, B.; Wolpert, D.; Xie, D.P.; Yildiz, Y. Cyber-Physical Security: A Game Theory Model of Humans Interacting Over Control Systems. *IEEE Trans. Smart Grid* **2013**, *4*, 2320–2327. [CrossRef]
99. Zhang, Y.X.; Malacaria, P. Bayesian Stackelberg games for cyber-security decision support. *Decis. Support Syst.* **2021**, *148*, 113599. [CrossRef]
100. Shukla, P.; An, L.; Chakrabortty, A.; Duel-Hallen, A. A Robust Stackelberg Game for Cyber-Security Investment in Networked Control Systems. *IEEE Trans. Control Syst. Technol.* **2023**, *31*, 856–871. [CrossRef]
101. Shen, J.J.; Feng, D.Q. Stackelberg Interdependent Security Game in Distributed and Hierarchical Cyber-Physical Systems. *Secur. Commun. Netw.* **2017**, *2017*, 9017039. [CrossRef]
102. Gao, B.Y.; Shi, L.B. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 30322–30331. [CrossRef]
103. Li, B.D.; Chen, Y.; Huang, S.W.; Yao, R.; Xia, Y.; Mei, S.W. Graphical Evolutionary Game Model of Virus-Based Intrusion to Power System for Long-Term Cyber-Security Risk Evaluation. *IEEE Access* **2019**, *7*, 178605–178617. [CrossRef]
104. Hu, H.; Liu, Y.L.; Chen, C.; Zhang, H.Q.; Liu, Y. Optimal Decision Making Approach for Cyber Security Defense Using Evolutionary Game. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 1683–1700. [CrossRef]
105. Huang, K.X.; Zhou, C.J.; Qin, Y.Q.; Tu, W.X. A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electron.* **2020**, *67*, 2371–2379. [CrossRef]
106. Kolokoltsov, V.N.; Bensoussan, A. Mean-Field-Game Model for Botnet Defense in Cyber-Security. *Appl. Math. Optim.* **2016**, *74*, 669–692. [CrossRef]
107. Miao, L.; Li, S. Cyber security based on mean field game model of the defender: Attacker strategies. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717737908. [CrossRef]
108. Miao, F.; Zhu, Q.Y.; Pajic, M.; Pappas, G.J. A hybrid stochastic game for secure control of cyber-physical systems. *Automatica* **2018**, *93*, 55–63. [CrossRef]
109. Miao, L.; Wang, L.N.; Li, S.; Xu, H.T.; Zhou, X.W. Optimal defense strategy based on the mean field game model for cyber security. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719831180. [CrossRef]
110. Orojloo, N.; Azgomi, M.A. A Stochastic Game Model for Evaluating the Impacts of Security Attacks against Cyber-Physical Systems. *J. Netw. Syst. Manag.* **2018**, *26*, 929–965. [CrossRef]

111. Singh, M.T.; Borkotokey, S.; Lahcen, R.A.M.; Mohapatra, R.N. A generic scheme for cyber security in resource constraint network using incomplete information game. *Evol. Intell.* **2023**, *16*, 819–832. [CrossRef]
112. Xing, W.; Zhao, X.D.; Basar, T.; Xia, W.G. Security Investment in Cyber-Physical Systems: Stochastic Games with Asymmetric Information and Resource-Constrained Players. *IEEE Trans. Autom. Control* **2022**, *67*, 5384–5391. [CrossRef]
113. Zhang, Y.C.; Liu, J. Optimal Decision-Making Approach for Cyber Security Defense Using Game Theory and Intelligent Learning. *Secur. Commun. Netw.* **2019**, *2019*, 3038586. [CrossRef]
114. Huo, Y.; Dong, W.; Qian, J.; Jing, T. Coalition Game-Based Secure and Effective Clustering Communication in Vehicular Cyber-Physical System (VCPS). *Sensors* **2017**, *17*, 475. [CrossRef] [PubMed]
115. Sanjab, A.; Saad, W.; Basar, T. A Game of Drones: Cyber-Physical Security of Time-Critical UAV Applications with Cumulative Prospect Theory Perceptions and Valuations. *IEEE Trans. Commun.* **2020**, *68*, 6990–7006. [CrossRef]
116. Sedjelmaci, H.; Brahmi, I.H.; Ansari, N.; Rehmani, M.H. Cyber Security Framework for Vehicular Network Based on a Hierarchical Game. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 429–440. [CrossRef]
117. Wu, Z.J.; Dong, R.C.; Wang, P. Research on Game Theory of Air Traffic Management Cyber Physical System Security. *Aerospace* **2022**, *9*, 397. [CrossRef]
118. Yang, Z.; Xiang, Y.P.; Liao, K.; Yang, J.W. Research on Security Defense of Coupled Transportation and Cyber-Physical Power System Based on the Static Bayesian Game. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3571–3583. [CrossRef]
119. Cone, B.D.; Irvine, C.E.; Thompson, M.F.; Nguyen, T.D. A video game for cyber security training and awareness. *Comput. Secur.* **2007**, *26*, 63–72. [CrossRef]
120. Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M.; Naqvi, S.A. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Trans. Softw. Eng.* **2019**, *45*, 521–536. [CrossRef]
121. Futter, A. *War Games* redux? Cyberthreats, US-Russian strategic stability, and new challenges for nuclear security and arms control. *Eur. Secur.* **2016**, *25*, 163–180. [CrossRef]
122. Harta, S.; Margheri, A.; Paci, F.; Sassonea, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Comput. Secur.* **2020**, *95*, 101827. [CrossRef]
123. Jin, Z.W.; Zhang, S.T.; Hu, Y.Y.; Zhang, Y.N.; Sun, C.Y. Security State Estimation for Cyber-Physical Systems against DoS Attacks via Reinforcement Learning and Game Theory. *Actuators* **2022**, *11*, 192. [CrossRef]
124. Kanellopoulos, A.; Vamvoudakis, K.G. Non-equilibrium dynamic games and cyber-physical security: A cognitive hierarchy approach. *Syst. Control Lett.* **2019**, *125*, 59–66. [CrossRef]
125. Maqbool, Z.; Aggarwal, P.; Pammi, V.S.C.; Dutt, V. Cyber Security: Effects of Penalizing Defenders in Cyber-Security Games via Experimentation and Computational Modeling. *Front. Psychol.* **2020**, *11*, 11. [CrossRef] [PubMed]
126. Nicho, M. Modelling serious games for enhancing end user cyber security awareness. *Iadis-Int. J. Comput. Sci. Inf. Syst.* **2020**, *15*, 91–106.
127. O'Connor, S.; Hasshu, S.; Bielby, J.; Colreavy-Donnelly, S.; Kuhn, S.; Caraffini, F.; Smith, R. SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security. *Inf. Sci.* **2021**, *580*, 524–540. [CrossRef]
128. Ravishankar, M.; Rao, D.V.; Kumar, C.R.S. A Game Theoretic Software Test-bed for Cyber Security Analysis of Critical Infrastructure. *Def. Sci. J.* **2018**, *68*, 54–63. [CrossRef]
129. Shah, P.; Agarwal, A. Cyber Suraksha: A card game for smartphone security awareness. *Inf. Comput. Secur.* **2023**, *31*, 576–600. [CrossRef]
130. Tseng, S.S.; Yang, T.Y.; Shih, W.C.; Shan, B.Y. Building a self-evolving iMonsters board game for cyber-security education. *Interact. Learn. Environ.* **2022**, *32*, 1300–1318. [CrossRef]
131. Yamin, M.M.; Katt, B.; Nowostawski, M. Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Comput. Secur.* **2021**, *110*, 102450. [CrossRef]
132. Yasin, A.; Liu, L.; Li, T.; Wang, J.M.; Zowghi, D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Inf. Softw. Technol.* **2018**, *95*, 179–200. [CrossRef]
133. Zeijlemaker, S.; Rouwette, E.; Cunico, G.; Armenia, S.; von Kutzschenbach, M. Decision-Makers' Understanding of Cyber-Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers. *Systems* **2022**, *10*, 49. [CrossRef]
134. Simon, H.A. *The Sciences of the Artificial*; MIT Press: Cambridge, MA, USA, 1969.
135. Hausken, K. Special Versus General Protection and Attack of Parallel and Series Components. *Reliab. Eng. Syst. Saf.* **2017**, *165*, 239–256. [CrossRef]