mathematics

MDPI

Review

Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review

Mohd Nor Akmal Khalid [1,2,*,†], **Amjed Ahmed Al-Kadhimi** [2,†] and **Manmeet Mahinderjit Singh** [2,†]

[1] School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi 923-1211, Japan
[2] School of Computer Sciences, Universiti Sains Malaysia, Georgetown 11800, Malaysia; amjed.alkadhimi@student.usm.my (A.A.A.-K.); manmeet@usm.my (M.M.S.)
* Correspondence: akmal@jaist.ac.jp
† These authors contributed equally to this work.

Abstract: Cybersecurity has become a prominent issue in regard to ensuring information privacy and integrity in the internet age particularly with the rise of interconnected devices. However, advanced persistent threats (APTs) pose a significant danger to the current contemporary way of life, and effective APT detection and defense are vital. Game theory is one of the most sought-after approaches adopted against APTs, providing a framework for understanding and analyzing the strategic interactions between attackers and defenders. However, what are the most recent developments in game theory frameworks against APTs, and what approaches and contexts are applied in game theory frameworks to address APTs? In this systematic literature review, 48 articles published between 2017 and 2022 in various journals were extracted and analyzed according to PRISMA procedures and our formulated research questions. This review found that game-theory approaches have been optimized for the defensive performance of security measures and implemented to anticipate and prepare for countermeasures. Many have been designed as part of incentive-compatible and welfare-maximizing contracts and then applied to cyber–physical systems, social networks, and transportation systems, among others. The trends indicate that game theory provides the means to analyze and understand complex security scenarios based on technological advances, changes in the threat landscape, and the emergence of new trends in cyber-crime. In this study, new opportunities and challenges against APTs are outlined, such as the ways in which tactics and techniques to bypass defenses are likely to evolve in order to evade detection, and we focused on specific industries and sectors of high interest or value (e.g., healthcare, finance, critical infrastructure, and the government).

Keywords: cybersecurity; attacks; behavior; network security; mobile; smartphone; trend; systematic review

MSC: 68M25

check for updates

Citation: Khalid, M.N.A.; Al-Kadhimi, A.A.; Singh, M.M. Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review. *Mathematics* **2023**, *11*, 1353. https://doi.org/10.3390/math11061353

Academic Editor: Sam Ganzfried

Received: 17 January 2023
Revised: 7 March 2023
Accepted: 8 March 2023
Published: 10 March 2023

1. Introduction

In the post-PC era [1], mobile and internet-of-things (IoT) devices have become ubiquitous, prompting sensitive and personal information to be moved into cyberspace [2]. For example, smartphones are involved in our daily activities and are used for countless purposes [3]. For instance, a trend in an organizations, known as "bring your own device" (BYOD), permits the use of personal computers and smartphones for corporate work [4,5], and in smart cities, personalized services adapt directions based on the user's health status [6]. The relevance of such trends and services is due to the expansion and evolution of various techniques that have blurred the boundary of cyberspace and the real world [7]. Such conditions lead to a plethora of cyber attacks that exploit various areas or "surfaces" of information via exposed or vulnerable heterogeneous elements [8].

As these kinds of devices are sophisticated devices that comprise multiple sensors (e.g., gyroscope, magnetometer, GPS, and microphone) and offer a plethora of services, valuable information assets are stored that are either personalized or corporate-related, placing individuals and organizations at risk of becoming targets for cyber attacks [4]. In addition, the traditional design of security mechanisms relies heavily on cryptographic techniques and the secrecy of cryptographic keys and system states [9]. However, the landscape of system security has evolved considerably, and attacks have become more sophisticated, persistent, and organized over the years. As a result, attackers use arrays of tools, such as social engineering and side-channel information, making it a fertile ground for specialized, yet stealthy, cyber attacks that require non-generic approaches to counter them.

One of the prominent cyber-attack types that fits such a profile is the advanced persistent threat (APT), which can be defined generically as a human-targeted attack that relies not only on social engineering and information collection but also on a broad spectrum of attack vectors. While characterized by its sophistication and complexity, it deliberately persists over a long time, a strategic motivation that is intelligence-driven and stealth-based to avoid detection [10–14].

According to the National Institute of Standards and Technology (NIST), the Computer Security Resource Center (CSRC) [15] defined an APT as "an adversary with a wealth of expertise and resources that can create opportunities to achieve its goals by using multiple attack methods. Advanced persistent threat attacks repeatedly pursue their objectives over a long period of time; adapt to the efforts of the defenders to resist it; and are determined to maintain the level of interaction necessary to implement its objectives." APT has also been described as a sustained and targeted attack that seeks to compromise the confidentiality, integrity, and availability (CIA) of information [8,16].

Moreover, an APT could also leverage zero-day vulnerabilities to ultimately compromise a system without detection by the system administrator [17]. In the context of mobile devices (e.g., smartphones), APT attacks were defined by Zulkefli and Singh [4] as sophisticated data-leak attacks via social engineering that benefit from their reliance on sensors (e.g., inertial, positioning, and ambient) and services (e.g., telephony, telecommunication, and utilities) that support information management.

Recently, game theory has had a growing number of applications in cybersecurity, where it has been utilized to better understand attackers and, consequently, to slow their progress. In addition, approaches underscored by game theory were able to develop a predictive model of human behavior for both targets and attackers [18]. A common assumption in standard game-theory models is that players are rational, and their goal is to seek an optimal strategy in the form of a Nash equilibrium [19].

The rationale of adopting game theory for APTs represents a paradigm shift from focusing on perfected preventive security measures to a strategic plan and the design of security mechanisms capable of adapting and mitigating losses over time. Such a situation can be achieved by modeling the interactions between a stealthy attacker who attempts to advance at each stage of the game and the system admin/designer attempting to detect and thwart the attack from reaching critical assets through a zero-sum game. This approach has featured the dynamic behaviors of APTs and their dynamic interactions between different layers and/or stages of the system, allowing for automated adjustments and responses, leading to more effective protection [9].

Previous review studies have made significant contributions to the cybersecurity field (Table 1). For instance, possible enhancements on threat-modeling approaches for sophisticated attacks, such as the APT, were outlined in Tatam et al. [20]. The review identified the complexity of the current systems, which require a hybrid approach to threat modeling and the visibility of the threats at all stages and levels. However, there is no one threat-modeling approach that can account for every situation. Therefore, Xing et al. [15] discussed the progress of detection and defense strategies against APTs using social engineering, machine learning, and anomalous flow-based methods. Defensive strategies using game theory were identified, including limited resources, dynamic information flow tracking, and cloud platforms.

Table 1. Summary of the differences between the current review and previous review studies.

References	APT Studies?	Game Theory?	Review Scope
Tatam et al. [20]	Yes	No	Threat and visibility modeling of complex security system
Xing et al. [15]	Yes	Yes	Progress of general strategies in detection and defense against APTs
Hejase et al. [21]	Yes	No	Descriptive analytics of APT awareness and its institutional impacts
Stojanović et al. [22]	Yes	No	Dataset creation, machine learning feature extractions, attack models, and detection system
Bhat and Kumar [23]	Yes	No	Analysis of bibliometric indicators to establish common research themes and aggregated communities
Kumar et al. [8]	Yes	Yes	Application-based and metric-based classification that balance between security, cost, and usability
Khaleefa and Abdulah [24]	Yes	No	Monitoring, detection, mitigation, and essential datasets classification
Jabar and Mahinderjit Singh [16]	Yes	No	Situational awareness modeling and behavioral monitoring with a proposed conceptual framework
This review	Yes	Yes	Trend and development, as well as benefit and challenges of game-theory approaches in APT detection and defense

Moreover, the awareness of APTs and their institutional impact according to descriptive analysis were reported in Hejase et al. [21], according to the secondary data reported in books, journals, websites, and blogs. Furthermore, Stojanović et al. [22] reviewed the literature concerning datasets and their creation for APT detection, particularly where machine-learning algorithms were utilized, and the study focused on the description and analysis of existing feature-extraction methodologies, attack models, and their relevance to network-based, cyber–physical-based, and anomaly-based intrusion-detection systems.

Furthermore, Bhat and Kumar [23] performed a bibliometric analysis of 1205 peer-reviewed articles on APTs from 2010 to 2020, from multidisciplinary perspectives, and common research themes and closely aggregated communities were reported based on bibliometric indicators (e.g., co-author graph, prolific authors, citation analysis, co-author analysis, and publication forums) and analyzed using an unsupervised Louvain algorithm.

In addition, Kumar et al. [8] provided critical reviews of application-based and metric-based classifications of game-theory approaches, which has potential for promoting objective decisions concerning countermeasures against APTs that consider the balance among security, cost, and usability. This review outlined the limitations of using game theory, including its assumptions about the behaviors of the parties involved and the complexity of analyzing large-scale games with many players. The study provided valuable insights into APT behavior, supported resource-optimal decision-making, and highlighted the importance of integrating practitioner perspectives to improve the risk management of information security.

The research in Khaleefa and Abdulah [24] provided detailed accounts of APT usage based on term definitions, its methodology, and classifying APT defensive strategies, which included monitoring, detection, and mitigation. Furthermore, the technical background of current APT detection and mitigation procedures, evaluation procedures of effective defensive strategies, the classification of an essential dataset, and the current state of progress in this field were described. Finally, Jabar and Mahinderjit Singh [16] provided a systematic literature review of 112 papers published from 2011 to 2022 that focused on various defense mechanisms to protect against APTs, including traditional security solutions and more advanced approaches, such as machine learning. A situational-awareness model, namely the observe-orient-decide-act (OODA), was introduced, which is a practical conceptual model for monitoring device behavior and mitigating APTs.

1.1. Practical Motivation

Between November 2021 and October 2022, ransomware Trojans attacked 271,215 unique users, including 77,256 corporate users and 8931 users associated with small- and medium-sized businesses [25]. During the reporting period, more than 23,807 ransomware modifications and 41 new families were identified. In addition, the emerging trend of electronic communications that take advantage of the internet through networked, mobile, and heterogeneous devices (i.e., the internet of things) was noted. As a result, addressing cyber attacks requires more than traditional defenses to resist known threats since it is no longer sufficient to protect against the exploits and the plethora of attack vectors [10].

When APTs were first identified, this initiated an arms race between APTs and cybersecurity organizations, and various vulnerabilities, defenses, detection methods, assessments, and awareness-based solutions have been identified. As a result, several APT case studies were found in the literature (see Table 2). However, current game-theory-based approaches for addressing APTs require in-depth investigation, while the APT trends, benefits, and challenges remain poorly understood.

1.2. Theoretical Motivation

Research conducted on APTs has utilized game theory for its capability to analyze the effects of attacks and defensive actions related to cybersecurity in various information and communication environments throughout society [26]. However, there remains a gap in the comprehensive understanding for quantifying the effects of behaviors and their implications for performance, organization, and security, in general.

A game comprises three essential elements: the players, action, and payoff. Determining the players and their payoff based on their actions and behaviors are the essential elements of game theory. However, a challenge arises when applying a game-theory approach to cybersecurity, as many variables exist that have to be considered, such as the system structure, the parties involved, network configuration environments, and the use of security assets and resources. Reliability, objectivity, and safety are the assessment criteria elicited through the various combinations and permutations that form the game-theory elements. A systematic literature review (SLR) was conducted to identify these elements.

1.3. Research Questions and Contributions

To this end, our study aimed to understand the prospective trends of game-theory approaches in the defense against APT attacks, where the target domain for future research and investigation was identified. This study was interested in identifying the answers for the following research questions:

1. What are the trends in current game-theory approaches (i.e., models, strategies, and features) that have been identified in the last half of this decade (2017–2022) for APT detection and defense?
2. What are the major benefits and challenges of adopting game-theory approaches in APT detection and defense?
3. What are the implications and converging topics for future research concerning APT detection and defense?

In summary, the key contributions of this study are, as follows:

- This study conducts a systematic literature review of game-theory-based approaches that have been identified in the last half of this decade (2017–2022) for APT detection and defense.
- This study outlines the latest trends that illustrate elements and factors that improve the application of game theory in cybersecurity.
- This paper also leverages the benefits and challenges of adopting game-theory approaches to identify the implications and converging topics for future research concerning APT detection and defense.

2. Theoretical Background

2.1. Advanced Persistent Threats (APTs)

APTs refer to malicious and well-thought-out cyber attacks by highly skilled actors with objectives that are strategically or operationally motivated [27]. They focus on particular businesses for long-term network access and employ tactics, techniques, and procedures (TTP) that are challenging to detect. APTs originated as a military term for attacks conducted by nation-states, and the term has been adapted and expanded to the information-security context by [5,16,27,28], as follows:

- Advanced: The adversary is accustomed to advanced infiltration tools, exploiting vulnerabilities, and may be multi-staged, and they intend to complete a task, instructions, or specific goals.
- Persistent: The adversary is stealthy and evasive with a long-term focus, as well as organized, well-resourced, and highly motivated.
- Threat: The adversary attacks cause either sensitive data loss or impede critical components, leading to considerable, and sometimes irreparable, damage.

As APTs pose a severe threat to modern society, several APT campaigns have been identified (Table 2), and these have raised significant concerns in cybersecurity and elevated the adoption of various effective APT detection and defense strategies. APTs typically involve targeted human-focused attacks, and thus they rely on social engineering, information collection, and a broad spectrum of attack vectors [10–14].

APTs have also been characterized by their sophistication, stealth, and complexity that is deliberately persistent over a long time period with an intelligence-driven strategic motivation. In summary, APTs have been used against different targets and organizations, where stealthy attack techniques were applied that evolved from stealing, exploiting, and compromising to more advanced techniques, including masquerading, social engineering, and deception, which has made it more difficult to design detection and defense mechanisms against APTs.

Table 2. Several APT case studies.

APT Campaign	Brief Descriptions
Titan Rain [28]	From 2003 to 2005, a series of coordinated cyber attacks that infiltrated a U.S. defense contractor's resources with the goal of stealing sensitive data concerning multiple attack vectors
Hydraq [28]	"Operation Aurora," involving a coordinated attack lunched in 2009 that used several malware components that were encrypted in multiple layers to remain undetected using the zero-day exploit in Internet Explorer
Stuxnet [29]	In June 2010, physically destroying part of the critical infrastructure (approximately one-fifth of nuclear centrifuges in Iran)
RSA SecureID Attack [28]	In 2011, a sophisticated cyber attack involving the compromise of information by installing a backdoor for remotely accessing an employee's machine and then harvesting the credentials of employees in an effort to reach the target system
Duqu [30]	In October 2011, a malware with striking similarities to Stuxnet, aimed at information collecting malware used for cyber-espionage
Flame [31]	In May 2012, "Flame" (at the time known as sKyWIper), an information-collecting malware using advanced spreading techniques masqueraded as a proxy for a Windows Update
Carbanak [28]	From 2013 to 2014, a cyber attack infiltrated the internal network of target banking/financial institutions through spear-phishing attacks to steal money
Red October [32]	Compromised the network systems of a large number of diplomatic, governmental, and scientific research organizations to steal credential data from various countries around the world

Table 2. *Cont.*

APT Campaign	Brief Descriptions
Naikon APT [33]	Targeted governments around the South China Sea in 2010–2015 used a bait document disguised as a Microsoft Word file to install spyware through a malicious executable
WannaCry [34]	A zero-day ransomware that caused world-wide catastrophes, from taking the United Kingdom National Health Service hospitals offline to shutting down the Honda Motor Company in Japan and demanded ransom payments to unlock the infected systems once it was activated
SolarWind [35]	Attackers smuggled malware within a legitimate signed update of SolarWind's sets of network and infrastructure monitoring services, acquiring high-level privileges and polluting authentication infrastructures
ZeroCleare [36]	Established trust and privilege given to signed binaries by system protections, such as a signed driver, to bypass a Windows hardware abstraction layer causing significant damage to energy and industry organizations in the Middle East
BlackEnergy [37]	In the summer of 2014, a BlackEnergy malware targeted Ukrainian governmental organizations for information harvesting

Every APT campaign behaves differently, and attacks are tailored to a particular victim or organization [16,27]. Typically, the first stage in an APT attack is establishing a point of entry into the network after gathering the necessary target information [5,8,38–40] (see Figure 1). After that, malicious software explicitly made for a target establishes a communication network through which attackers can introduce malicious code. This malicious software sneaks through the system laterally, seeking security vulnerabilities that it can use to infect other network systems (second stage). The malicious software also copies itself to maintain persistence inside the targeted system. As a result, APTs can create new connections by conducting surveillance until they succeed in disrupting the targeted system and steal data (third stage).

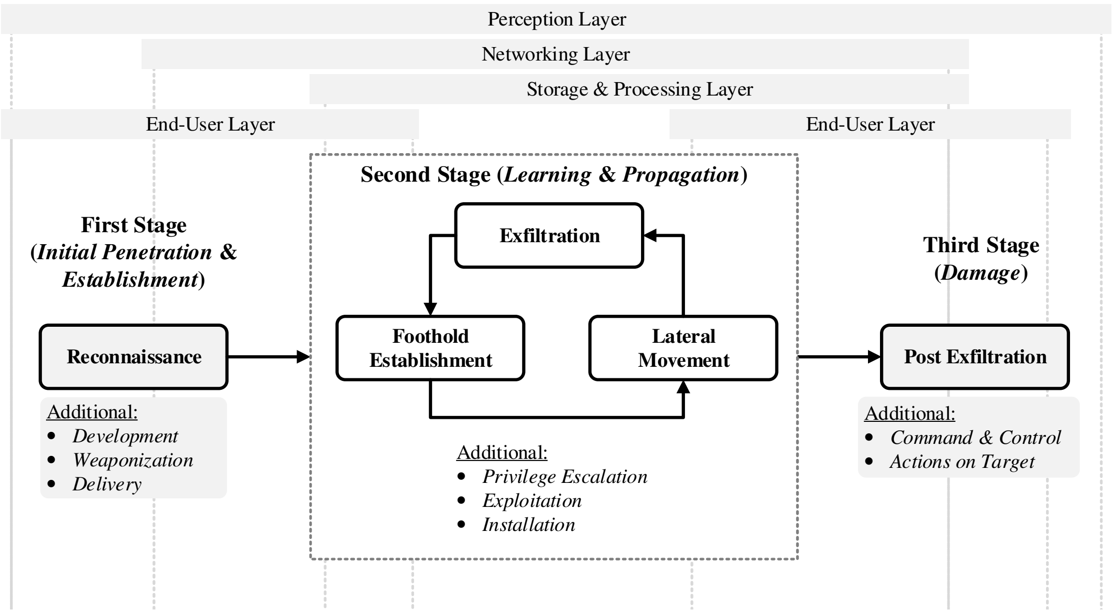

Figure 1. Advanced persistent threat (APT) attack stages (adapted from [8,38–40]), where some stages may have concurrent/parallel steps. The APT stages may be supplemented with additional steps/procedures to compensate for emerging technologies and defense mechanisms [38,39]. The boundary between physical and virtual layers may also be crossed between the APT stages, depending on the attack behaviors and target system [40].

Some industry standards, practitioner manuals, and vulnerability catalogs are available, including the NIST ICS guidelines [41], CAPEC [42], NVD CVSS [43], ATT&CK [44], and RISI [45]. These catalogs of threat and vulnerability patterns serve as a shared knowledge repository for current and future APTs. However, the study and development of solutions against APTs should be more cohesive within the literature, as workable and failed solutions have been inconsistently reported and described. Therefore, this systematic literature review was focused on niche solutions for detecting and defending against APTs.

2.2. Game Theory in Cybersecurity

2.2.1. Brief History and Classification

The strategic interaction between competing or cooperating interests where the limitations and payoff for actions are considered define a game [46]. Furthermore, a player is a fundamental character in a game who must decide on a course of action. A player may be a person, a machine, or a collection of people in a game. According to game theory, situations involving multiple players involve games in which each participant makes decisions that maximize their rewards while anticipating the rational choices of the other participants.

Since the seminal work by Van Dijk et al. [47] proposed a game theory formulation to address the APT challenge, other studies have followed suit. Game theory has been used to investigate the mathematical models of conflict and cooperation between rational and intelligent decision makers [48]. It offers a sophisticated framework for comprehending the characteristics of APTs, such as stealth and uncertainty. Since attacker incentives, defense resource allocations, and attack impacts are all subject to constraints, game theory is a logical choice for the formal reasoning of strategic interactions.

Game theory has a long and varied history in the field of security, from the design of real-time military systems (e.g., those used for missile interception) to promoting strategic choices regarding substantial defense investments and acquisitions [49]. Two causes have contributed to this condition. First, by framing it in quantitative terms, such as a payoff, cost, gain or loss, and risk, game theory offers a natural framework to quickly translate a high-level policy decision into the best course of action. Decision-makers have a unified basis to support making a particular choice. Second, it offers a rigorous mathematical framework for analyzing and maximizing various scenarios following predetermined criteria. As a result, this evaluation has frequently been a crucial factor in successful security operations and enabled superior decision-making under time constraints.

In cybersecurity, the strategic interaction between two players, in which each attempts to maximize their interests, was outlined by game theory to determine the defender's response to their attacker, and vice versa [50]. The tactics of both the defender and the attacker heavily influenced the opposing side. Therefore, both the defender's and the attacker's strategic actions affected the effectiveness of a defense mechanism. The game-theory approach was used to conduct a tactical analysis of various attack vectors. Furthermore, game theory has been used to investigate the defender's strategic decision-making contexts and assess the attackers' incentives. Thus, game-theory approaches have provided several key advantages [49,50]:

1. Proven mathematics: Heuristics are used in most traditional security solutions, whether implemented in proactive (e.g., firewalls) or reactive (e.g., anti-virus programs) hardware. Game theory, however, methodically and mathematically investigates security choices.
2. Reliable defense: Based on the game's analytical results, researchers can create defense mechanisms for reliable cyber-systems to be used against self-centered behaviors (or attacks) by malicious users/nodes.
3. Timely action: Adopting traditional security solutions may be faster because these methods do not consider the incentives for participants. Game-theory approaches support defenders by using underlying incentive mechanisms to allocate limited resources in order to balance the perceived risks.

4. Distributed solutions: Instead of making decisions on an individual (or distributed) basis, most traditional defense mechanisms use a centralized model. However, the need for a coordinator in an autonomous system makes the centralized approach in a network security game challenging. Therefore, security solutions using the appropriate game models are required for distributed systems.

2.2.2. Game Concepts and Nash Equilibrium

A solution is a methodical explanation of the game-play using the optimal strategies possible and predicting the results. The *consequence* function links an outcome to each executed decision. Furthermore, a preference relation links together the consequences that model each player's preferences in a game. Finally, a player's strategy is a comprehensive action plan for all potential game scenarios. A pure strategy calls for a specific course of action in a given set of circumstances. A mixed strategy is when the plan specifies a probability distribution for every action that could be taken based on a given set of circumstances.

The Nash-equilibrium point is a critical concept in game theory. The intersection of the best responses, or when each player is playing in response to another player's actions, is known as a Nash equilibrium [46]. No player would choose to change their strategy because doing so would reduce their payoffs, assuming that all other players follow the recommended strategy, which is defined as the Nash equilibrium [48,50]. This concept describes the steady-state condition of the game. However, it only describes the steady state; it does not consider the methods by which the game reaches that steady state. Numerous other concepts exist; however, the Nash equilibrium is the most well-known.

A Pareto-efficient Nash equilibrium, another well-known game concept, is only occasionally valid. A strategy profile is Pareto efficient if no player can raise their payoff without lowering another player's payoff [50]. Every game is based on two key ideas: Common sense and rationality [46]. The likes and dislikes of each participant in a game are disregarded by rationality, which is required for consistent decision-making. Instead, both prior knowledge of the results and the shared understanding of each player regarding the results comprise common knowledge.

2.2.3. Game-Theory Types

The interaction between malicious attackers and defenders was modeled using game-theory methods. In addition, different game types have been examined regarding how the defender and attacker act. Finally, some key elements that categorize the various mechanics of games in the context of cybersecurity have been discussed, as follows [50]:

- Complete versus incomplete information: All players' payoff functions and strategies are known in a complete information game. However, in a game with incomplete information, at least one player cannot observe another player's payoff mechanisms and game plans. Therefore, we can use Bayesian rules to foretell the game's outcome.
- Perfect versus imperfect information: A game is referred to as a perfect information game if each player can ascertain the strategies selected by other players after each step. In a game with perfect information, each player can see every other player's previous move after it is made. However, with incomplete information, it is not possible to accurately predict the action of other players in a game. Therefore, players can only apply stochastic methods to a noisy observation of the past behaviors of other players.
- Static: The players are thought to make their own decisions simultaneously in a static game (e.g., strategic game). Static prisoner's dilemma games (PDGs), zero-sum games, and Stackelberg games are typical static security games. Even if a player makes an unreasonable action, the best choice may still be made (Nash equilibrium has no Pareto efficient in a one-shot game). Players' cooperation may develop in subsequent games to achieve the anticipated future gains.
- Dynamic: This is a game with numerous levels that are created by repeatedly playing a static game, definitely or indefinitely. A common strategy for arriving at a sub-

game-perfect equilibrium, the standard resolution of a dynamic game, is through backward induction. An instance of a dynamic game is a repeated game having two categories: Perfect and imperfect information. If one player can observe the tactics used by other players, then a repeated game is the perfect information game. The players' pure strategy in the repeated game corresponds to the current stage's strategy for all possible game histories. Therefore, even though it might not be Pareto efficient, it is best to play a game according to the Nash equilibria of the stages in finite repeated games if the total number of stages is known.

- Stochastic: This is also derived from dynamic games. Stochastic games transition from one stage to another according to the transition probabilities. The game's stages occasionally change deterministically or randomly, depending on the past behavior of a fixed group of players. The likelihood of the present state is typically influenced by the past state and the players' actions. The stochastic game repeats with random states when the current state is unrelated to the previous state and players' actions. The Markovian game is a specific type of stochastic game. Its state-changing process is a Markov process (i.e., probability distribution on the next state is determined only by the previous state and actions). Nash equilibria are obtained in a Markovian game using the solution of a chain of Markov-decision processes.
- Evolutionary: The model population changes over a long period, similar to the selection and mutation occurrences in the natural world. Mutations increase population diversity, whereas selection favors some varieties over others. Players are presumed to be rational in general game theory; however, this assumption is relaxed in evolutionary game theory. Due to this circumstance, a few mutants may use irrational tactics to win an evolutionary game. Players are not assumed to be familiar with the game in a large population. Instead, players attempt to increase their self-interest or the average number of surviving offspring. The mutagenic evolutionary stable strategy (ESS) is the standard equilibrium solution in evolutionary game theory. As a result, when using ESS, a population can remain stable over time.
- Non-cooperative versus cooperative: Players in a non-cooperative game-theory approach choose a plan of action to advance their interests. However, in a cooperative game, players work together to develop strategies that benefit both parties. Last but not least, a coalition game is a cooperative game in which players band together to achieve a shared goal. Players must coordinate their actions to form a coalition, and then they agree to split the coalition's total reward equally. In addition, an equilibrium of a coalition game should be resistant to any class of players deviating from an established game solution to ensure no players are motivated to change their coalition.

3. Literature Search Methodology

Our approach for conducting this literature survey study consisted of three stages: (1) information gathering, (2) article filtering, and (3) article reviewing. In the first stage, relevant search terms were identified from the topic of interest using seed words ("advanced persistent threat" and "game theory"), and relevant search terms were determined, where relevant research articles were extracted from the selected databases. In the second stage, the retrieved articles were filtered according to their titles and abstracts if they fulfilled either the inclusion or the exclusion criteria. Finally, the third stage focused on reviewing the content of each research article.

Five primary scientific databases were used to identify articles concerning APT studies that used a game-theory approach. The databases included the Scopus abstract and citation database, the Web of Science core collection, the ACM digital library, the IEEE Xplore digital library, and ScienceDirect. These databases provided a variety of peer-reviewed research articles relevant to artificial intelligence, human–computer interactions, cybersecurity, and mobile computing. The search strategy involved developing a search string with a strong connection to the terms related to the research questions and included synonyms of the search terms [51].

The initial search string used to query the selected databases was the seed search term "advanced persistent threat", which broadly described the target subject matter. Then, based on the articles identified using the seed term, the following search terms were used to narrow the scope of target topics and subjects: "game theory", "cybersecurity", "computer crime", "security", and "network security". In addition, additional search terms included "mobile" and "smartphone", where the application of the subject matter was found as well. Finally, all the search terms were searched for within the article titles, abstracts, and text (if available).

To ensure the quality of the publication sample, an initial screening was conducted to filter relevant articles based on: (a) articles that included the search terms related to the topics and subject matters; (b) articles published in peer-reviewed journals to ensure quality; (c) articles that provided access to the full text; (d) articles that were published in the English language (to ensure understanding); and (e) articles published within the past five years, excluding this year, during January 2017 to October 2022 (to ensure relevance). In addition, duplicate articles, such as those found in more than one database, were removed.

As a result of the initial screening, 123 papers were selected. Table 3 presents the results of the keyword search (and associated criteria) for each database. The literature search results based on content-related inclusion/exclusion criteria are presented in Table 4. At the end of the entire literature-selection procedure, a total of 48 articles were included in the final literature sample. Figure 2 presents the process of the online literature search using a PRISMA 2020 flow diagram [52].

Table 3. The results of the keyword search by scientific database.

Database	Initial Hits			Screening	Eligibility
Sources	(Keywords)	Initial	Typology	Scope	(Title and Abstract)
SCOPUS	297	177	68	52	25
WoS	18	10	8	5	4
ACM	156	103	4	3	2
ScienceDirect	109	59	20	18	10
IEEE Xplore	79	25	23	20	7
Total	659	374	123	98	48

Table 4. Inclusion and exclusion criteria for the relevant literature search (article filtering).

Inclusion Criteria	Exclusion Criteria
(a) Answered the research question (b) Only academic publications (c) Focused on APT-based investigation in security context (e.g., network and cloud storage, cyber–physical systems, and internet of things) (d) Focused on APT-based investigations using a contemporary game-theory approach (e) Only primary studies that included empirical results based on a specified research methodology	(a) Did not directly answer the research question (b) Non-academic publications (c) Focused on other aspects of APT-based investigations in security context (e.g., vulnerability studies, threat modeling, and risk management) (d) Focused on other aspects of APT-based investigations not using acontemporary game-theory approach (e) Studies, such as literature reviews and other APT-based investigations (e.g., vulnerability studies, threat modeling, and risk management)

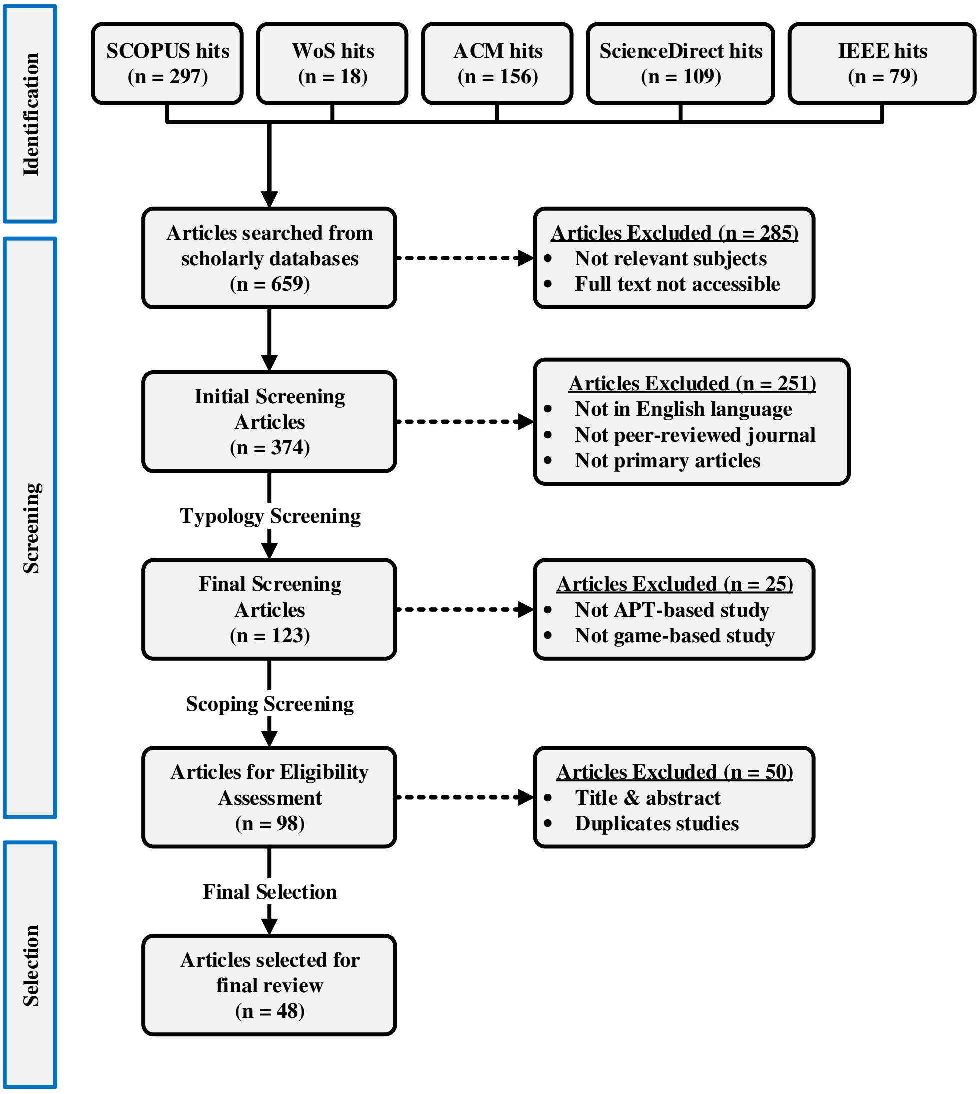
Identification
Screening
Selection
SCOPUS hits (n = 297)
WoS hits (n = 18)
ACM hits (n = 156)
ScienceDirect hits (n = 109)
IEEE hits (n = 79)
Articles searched from scholarly databases (n = 659)
Articles Excluded (n = 285)
• Not relevant subjects
• Full text not accessible
Initial Screening Articles (n = 374)
Articles Excluded (n = 251)
• Not in English language
• Not peer-reviewed journal
• Not primary articles
Typology Screening
Final Screening Articles (n = 123)
Articles Excluded (n = 25)
• Not APT-based study
• Not game-based study
Scoping Screening
Articles for Eligibility Assessment (n = 98)
Articles Excluded (n = 50)
• Title & abstract
• Duplicates studies
Final Selection
Articles selected for final review (n = 48)

Figure 2. PRISMA flow diagram for the selection of the 48 main articles reviewed. The initial search was identified from five major scientific databases, screened through several filtering criteria, and the final selection was determined from an eligibility assessment.

Finally, the considered articles were reviewed for information relevant to the goal and the research questions for further synthesizing. This process involved two essential steps [53,54]: (a) the extraction of data and (b) an evaluation and appraisal of the article quality. These steps were performed on the final 48 articles, and they were reviewed and guided by an extraction form developed according to two models [55], which accommodated the multidisciplinary character of the current study. These models originated from two different but interrelated focuses in the security field: detection and defense.

The extraction form was developed to identify and organize important, relevant information in the reviewed articles while evaluating and determining their quality. For these purposes, the extraction form included information, such as the article identification data (i.e., title, journal, author, origin of authors, year of publication, and publication source) as well as detailed information regarding both methodological considerations and the results of the study. Therefore, based on the extraction method of Nicolescu and Tudorache [54], Table A1 presents the extraction method used in the present study for the information synthesis and the quality evaluation of the considered articles.

A detailed presentation of the methodological organization and data analysis methods was used as a dichotomous criterion to evaluate the quality of the studies and accept them for the final sample. The publication sample included articles that had described their empirical findings in detail and studies with empirical results related to our research questions (i.e., APT detection and defense). All publications in the final sample underwent a synthesizing procedure to determine the converging trends by aggregating, discussing, organizing, and comparing the selected publications; tabulating their study samples; and highlighting recurrent topics for future works, which followed the narrative synthesis (c.f., further on the topic of narrative synthesis by Okoli [53]).

4. Results and Discussion

The present narrative synthesis included two types of analyses: (a) an empirical description of the publications selected for review (e.g., countries, frequencies, years, and subject category) and (b) the thematic analysis of the publications according to the research questions and based on the proposed theoretical framework.

4.1. Descriptive Analysis–The Organization of the Studies

The descriptive analysis presented the results from evaluating 48 articles that empirically investigated APT detection and prevention using a game-theory approach, according to (a) the year of publication, (b) the countries of origin where the empirical research was conducted, (c) the subject domain of the publication sources, and (d) the industries involved in the studies.

The increased development of APT detection and prevention methods using a game-theory approach (after 2018) as well as the increased use of game theory, overall, was reflected in the increased research interest in this topic—approximately 77% of the articles were published between 2019 and 2022 (Figure 3). Further investigation of the topic is expected in the future, as the use of game-theory approaches for the detection and prevention of APTs is likely to steadily increase. The industrial application of the game-theory approach in APT detection and prevention was primarily utilized in the field of enterprise networks, cyber–physical systems (CPSs), and industrial control systems (ICSs), where this accounted for approximately 40%, 25%, and 21%, respectively, of the 48 published articles (Figure 4).

In addition, the secondary industrial application included cloud storage and the internet of things (IoT), which comprised approximately 38% of the 48 published articles. This indicated the importance of these emerging areas of the investigated topic. Other areas included network-related (e.g., fog, wireless, and mobile computing) and utility-related (e.g., smart home, power grid, and data recovery) applications for addressing APTs using a game-theory approach, accounting for approximately 23% of the 48 published articles.

Most articles (94%) were authored by researchers from the United States of America (U.S.) and China, while authors from Australia, Austria, and South Korea were the second highest (approximately 21%). In addition, based on the years considered, although the U.S. had the highest number of publications between 2017 and 2020, authors from China published the highest number in 2021. Cumulatively, approximately one-third of the empirical research (approximately 29%) were conducted in European, Middle Eastern, and Asian countries (Table 5). This indicates that the application of game-theory approaches has increased in other countries, apart from the U.S. and China, and multiple countries have investigated this approach to APT detection and prevention.

The major venues of publication were represented by journals from the subject domains of computer science and information systems (Figure 5), at 75% and 44%, respectively, of the published articles. Moreover, subjects, such as multidisciplinary sciences, theory and methods, and engineering were also main subjects of focus among the journals, accounting for approximately 25%, 19%, and 19%, respectively, of the articles published. In addition, these five subject categories reflected the majority of the output, accounting for approximately 42% and 67% out of the total output during 2020 and 2021, respectively. This indicates that APT topics using a game-theory approach were not limited to computing-related fields but were also useful in theoretical works and other complementary fields (e.g., business and service).

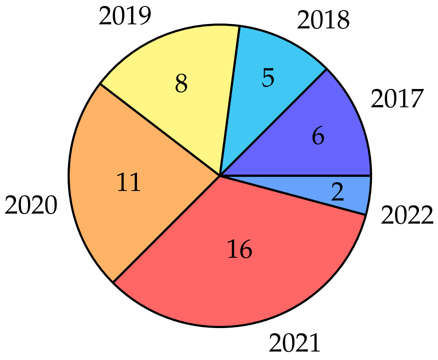

Figure 3. Publication by year (for the 48 total articles).

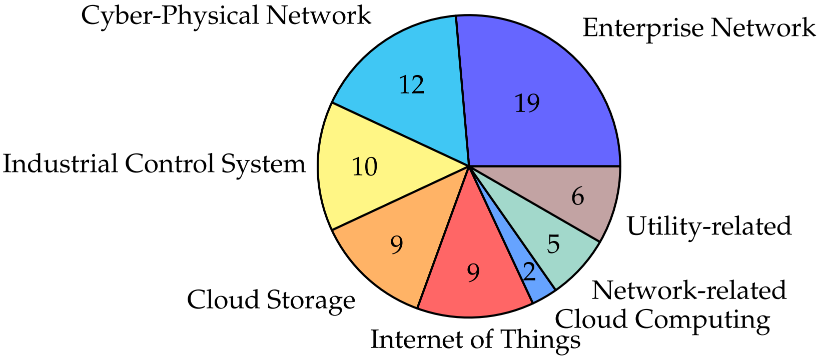

Figure 4. Publication by industrial application area (for the 48 total articles).

Table 5. Publication country of origin aggregated by their year of publication (note: one publication may be attributable to multiple countries).

Country	2017	2018	2019	2020	2021	2022	Total
China	2	3	4	5	8	1	23
U.S.	5	4	4	5	3	1	22
Australia	0	0	1	1	2	0	4
Korea	0	1	0	0	2	0	3
Austria	2	1	0	0	0	0	3
Canada	0	0	0	0	2	0	2
Germany	1	0	0	0	1	0	2
U.A.E.	0	0	0	0	1	1	2
Pakistan	0	0	1	0	0	0	1
U.K.	0	0	0	0	1	0	1
Singapore	0	0	0	0	1	0	1
Macau	0	0	0	0	1	0	1
Spain	0	0	0	0	1	0	1
Iraq	1	0	0	0	0	0	1
Czech Rep.	0	0	1	0	0	0	1
New Zealand	0	0	0	0	1	0	1

Furthermore, other important publication venues were represented by journals from the fields of telecommunications, engineering, and automation and control systems, which demonstrated the topic's relevance to specific industries (e.g., control systems, engineering processes, and communication media/networks). Some publication venues had little relevance to the topic as they were focused outside of computing-related fields; however, they emphasized the broad implementation of game-theory approaches (for instance, applying a game-theory approach to the prevention of APT attacks on the internet of vehicles [56]). Finally, the highest publication distribution in the different subject categories was observed in 2021, where approximately 90% of the publication output was found.

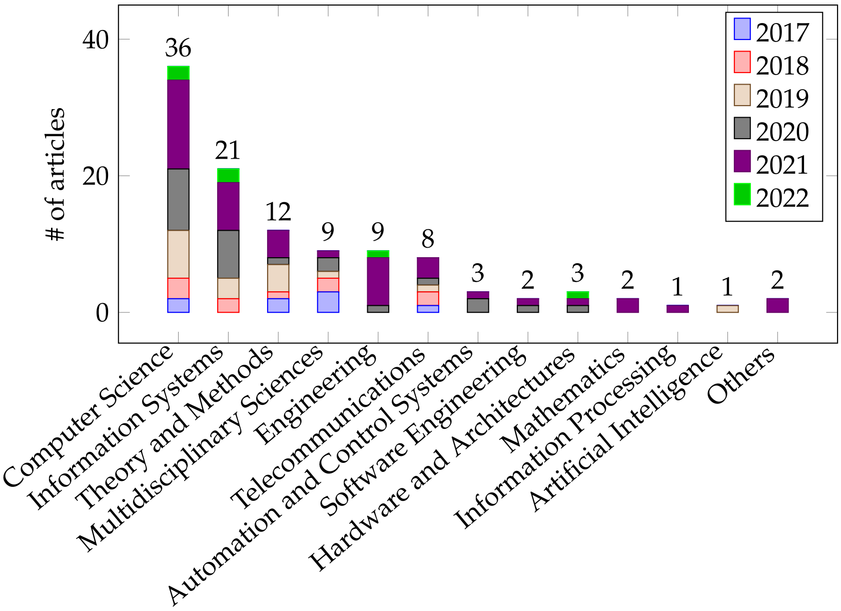

Figure 5. Subject domain of the publication sources of the included articles (note: one publication may be attributable to multiple subjects, and one source may have more than one subject domain).

4.2. Thematic Analysis—Narrative Description

Based on the search and extraction methodologies described in Section 3, a comprehensive analysis and evaluation of the 48 selected articles was conducted, relating to the three research questions presented at the end of Section 1. The narrative intention of this study focused on the frequency of the themes and elements throughout the studies. The themes commonly found in all the studies were centralized on detection and defense modalities against APTs. Furthermore, the context of these modalities was investigated, and the common focus between the considered studies was outlined. Subsequently, several elements of APT approaches in the considered studies involved the detailed design of their game-theory methodology, such as the game process, game types, game structure, and game strategies.

4.2.1. Current Trends of Game-Theory Approaches in APT Detection and Prevention

The current trends of game-theory approaches for addressing APTs are summarized in Table 6. Overall, the approaches were diverse and provided significant coverage of the different APT studies. Most of the studies focused on the objective of APT detection through increased awareness, including [26,32–34,36,38–40,56–90]. Most of them adopted multi-stage game processes to model the adversarial interactions between the attackers and the defenders (or multiple entities) and differentiated between different levels (or phases) and timing (or circumstances) [56–58,63,68,71,73,81,84,87,88,90].

In addition, some studies adopted mixed strategies to solve these game processes and reach an optimal payoff equilibrium, depending upon the perspective of the game state (defender or attacker point-of-view) by improving the possible outcomes through randomizing the moves made [56,57,81,84,90]; however, some studies employed pure strategies when the best payoffs were the only options determined to achieve the maximum profit or the best outcome [87,88].

Table 6. Summary of game-theory approaches for APT detection and prevention, aggregated by objectives, game features, and added values.

		Objective								**Game Features**														
		Defense			**Detection**			**Proc.**		**Type**							**Struct.**		**Strategy**					
Ref.	**Year**	**Improvement**	**Mitigation**	**Vulnerability**	**Awareness**	**Performance**	**Prediction**	**Single-Staged**	**Multi-Staged**	**Static**	**Dynamic**	**Markov**	**Bayesian**	**Signaling**	**Gaussian**	**Stochastic**	**Two-player**	**N-player**	**Pure**	**Mixed**	**Hybrid**	**Gestalt**	**Stackelberg**	**Added Value**
Xiao et al. [91]	2017	✓						✓				✓					✓		✓	✓				PT
Rass et al. [92]	2017		✓					✓								✓	✓			✓				Attack tree/graph
Abass et al. [93]	2017					✓	✓		✓		✓							✓	✓	✓				ESS, resist small perturbations
Rass et al. [57]	2017				✓				✓		✓							✓	✓	✓				BR
Chen and Zhu [32]	2017			✓					✓		✓						✓			✓				FlipIt, Contract theory
Pawlick and Zhu [58]	2017	✓			✓		✓		✓		✓			✓				✓				✓		FlipIt
Xiao et al. [59]	2018					✓			✓		✓						✓		✓	✓				Cumulative PT, PHC
Min et al. [60]	2018				✓	✓		✓								✓	✓			✓				CBG, Strict resource, PHC
Lee et al. [26]	2018			✓	✓			✓		✓							✓		✓					Attack tree/graph, CVE
Huang et al. [61]	2018					✓			✓		✓	✓					✓		✓					DG
Zhu and Rass [38]	2018	✓					✓		✓		✓		✓					✓				✓		Multi-layer Nested games
Laszka et al. [62]	2019		✓				✓		✓						✓		✓		✓					AD, SA
Lv et al. [63]	2019				✓	✓			✓		✓							✓			✓			Data fusion
Yang et al. [64]	2019		✓	✓					✓		✓						✓		✓					Repair Problem, ESS, DG
Pawlick et al. [33]	2019	✓		✓					✓		✓			✓				✓				✓		FlipIt, OC
Pawlick et al. [65]	2019			✓	✓			✓			✓			✓			✓		✓	✓				Cheap-talk, DD
Li and Yang [66]	2019		✓			✓			✓		✓						✓		✓					DG, PT
Wang et al. [67]	2019	✓							✓			✓	✓			✓	✓		✓	✓				NLP
Horák et al. [68]	2019				✓		✓		✓		✓	✓				✓	✓		✓					Lateral movement, Attack tree/graph
Huang and Zhu [39]	2020			✓			✓		✓		✓		✓				✓		✓					Belief system, DP, DD
Moothedath et al. [69]	2020		✓			✓	✓		✓		✓						✓			✓				IFT
Yang et al. [70]	2020		✓			✓		✓			✓		✓				✓						✓	Greedy solver, DG
Li et al. [71]	2020	✓			✓			✓			✓			✓			✓				✓			Anti-HP
Zhang et al. [72]	2020	✓		✓					✓		✓	✓					✓			✓			✓	Strict resource, DP
Zhang and Zhu [73]	2020			✓	✓				✓		✓					✓		✓	✓					FlipIt, Insurability concept, TSS
Gill et al. [40]	2020				✓	✓		✓		✓							✓			✓				SD, AD, HP

Table 6. *Cont.*

Ref.	Year	Objective						Game Features																Added Value
		Defense			Detection			Proc.		Type							Struct.		Strategy					
		Improvement	Mitigation	Vulnerability	Awareness	Performance	Prediction	Single-Staged	Multi-Staged	Static	Dynamic	Markov	Bayesian	Signaling	Gaussian	Stochastic	Two-player	N-player	Pure	Mixed	Hybrid	Gestalt	Stackelberg	
Bakker et al. [74]	2020			✓				✓			✓						✓			✓				Tractable NLP
Hu et al. [34]	2020					✓	✓		✓		✓					✓		✓		✓				ESS, BR
Tan et al. [75]	2020	✓	✓						✓		✓						✓			✓				SIRM, CKC, MTD
Tian et al. [76]	2020				✓	✓		✓		✓			✓				✓		✓					HP, PT, BR
Ye et al. [77]	2021		✓	✓				✓					✓			✓	✓			✓				Differential privacy, DD
Xie et al. [78]	2021	✓					✓		✓		✓	✓	✓				✓		✓					Attack tree/graph
Yang et al. [79]	2021	✓	✓						✓		✓						✓		✓					DG
Gao et al. [80]	2021	✓				✓			✓		✓							✓	✓					DG, Hamilton OC
Huang and Zhu [81]	2021			✓	✓				✓		✓		✓				✓			✓				Belief system, HP, DD
Feng et al. [82]	2021			✓		✓			✓		✓							✓					✓	OC, ESS, BR
Merlevede et al. [83]	2021	✓		✓					✓		✓					✓	✓				✓			FlipIt, Time discounting
Nisioti et al. [84]	2021				✓				✓				✓				✓			✓				Attack tree/graph
Tian et al. [36]	2021		✓	✓	✓			✓			✓						✓		✓					BR, HP, PT, ESS
Joshi et al. [85]	2021	✓			✓	✓		✓					✓					✓		✓				ARA, EUT
Bakker et al. [86]	2021		✓		✓			✓					✓	✓		✓		✓		✓				MG, HG, OC, BR, DD
Mi et al. [87]	2021		✓		✓	✓			✓							✓		✓	✓					DG, NIRM
Tan et al. [88]	2021	✓		✓	✓				✓		✓						✓	✓						FlipIt, DG, TSS, MTD
Halabi et al. [56]	2021	✓			✓	✓	✓		✓				✓				✓			✓			✓	Strict resource, ARA, MILP
Liu et al. [89]	2021			✓			✓	✓					✓				✓			✓				PN, TPM
Seo and Kim [90]	2021	✓		✓	✓				✓		✓	✓	✓			✓	✓			✓			✓	TSS, DD, Attack surface, MTD
Wan et al. [94]	2022	✓		✓			✓		✓		✓						✓				✓			HG, Belief system, CKC, DD, EUT
Li et al. [95]	2022	✓					✓		✓		✓		✓				✓						✓	Strict resource, DCNN

ARA: Adversarial Risk Analysis; NLP: Nonlinear Programming; MILP: Mixed-Integer Linear Program; DP: Dynamic Programming; TPM: Threat Propagation Matrix; BR: Bounded Rationality; ESS: Evolutionary Stable Strategies; CKC: Cyber Kill Chain; CVE: Common Vulnerabilities and Exposures; PHC: Policy Hill Climbing; PT: Prospect Theory; PN: Petri Net; EUT: Expected Utility Theory; AD: Anomaly Detection; SD: Signature Detection; DD: Deception Detection; HP: Honeypot; MG: Metagame; HG: Hypergame; DG: Differential Game; CBG: Colonel Blotto Game; IFT: Information Flow Tracking; SIRM: Susceptible, Infectious, Recuperate, Malfunctioned; NIRM: Normal, Infected, Restored, Malfunctioned; MTD: Moving Target Defense; TSS: Temporospatial Strategy; OTP: One-Time Password Mechanism; OC: Optimal Control (e.g., Hamilton); SA: Simulated Annealing; and DCNN: Deep Convolutional Neural Network.

Furthermore, many reviewed articles focused on identifying and detecting a potential vulnerability in their study domain (or industrial application) against APTs [33,38,56,58,67,71,72,75,78–80,83,85,88,90,91,94,95], whereas some more recent ones concurrently provided improvement techniques on their APT detection method to overcome these vulnerabilities [33,72,88,90,94]. While pure and mixed strategies were among those most used by researchers throughout the years (Figure 6), they also tended to be unrealistic and impractical due to the nature of APT stealth and human-focused attacks (e.g., irrational, unpredictable, and adaptive). Therefore, different strategies have been adapted by researchers to further enhance their game-theory approaches against APTs.

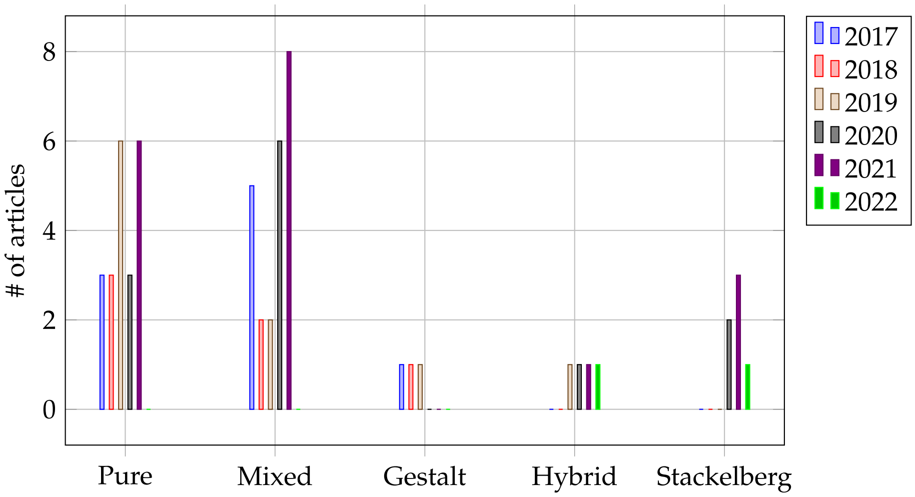

Figure 6. Publication output by year based on game-theory strategies against APTs.

Before the 2000s, a prominent approach was the Gestalt strategy, which was inspired by the psychological concept that a being is more than the sum of its experiences [96]. Such a strategy allowed for optimizing the equilibrium of a system with multiple phases (temporal) and stages (spatial) simultaneously in a way that was determined elegantly and holistically [38,58]. The strategy was also related to multi-layered games, and it required solving each game optimally, given the results of the other games, without the need to analyze one large game [33]. These multiple games or combinations of sub-games could be structural variants of games (i.e., signaling games and FlipIt games) that ensured that plug-and-play solutions were widely available.

Furthermore, several studies adopted hybrid strategies to address high-risk conditions in APTs [63,71,83,94]. This strategy involved judging the availability of multiple information sources (i.e., multiple levels and phases), ensuring different probabilities of choice [63] and managing the diversity of capabilities and opportunities [71], as well as belief systems [94]. In addition, when a critical resource was finite (e.g., time or cost), hybrid strategies were a vital advantage, relative to the timing of its deployment: for instance, fixed (a "periodic" strategy) and exponential (an "exponential" strategy). Under such conditions, specific decision-making could be costly over time and disincentivize adverse intentions [83]. Moreover, the hybrid strategy also provided diversity in resolving APT problems when conflicting information or uncertainty was present [94].

In recent years, Stackelberg's strategy was among the most popular strategies adopted in game-theory approaches to address APT problems [56,70,72,82,90,95]. It is based on the strategic leadership model in economics, where a leader and a follower compete on quantity by moving sequentially (sometimes referred to as the "market leader"). The purpose was to focus on minimizing potential loss or maximizing the payoff [70,72] when faced with an asymmetric information structure (i.e., stealthy attacks) by using randomized policies [56,72,90] and optimally allocating critical resources and judgments [82,90]. Moreover, the presence of a leader allowed for the discovery of high rewards that would not affect the equilibrium [56].

Considering the game processes of the game-theory approaches adopted against the APTs, seven distinct process types were identified from the reviewed articles (Figure 7): static, dynamic, Markov, Bayesian, signaling, Gaussian, and stochastic (refer to Section 2.2.3 for details). Among them, the Bayesian and stochastic game processes were frequently adopted, accounting for about 29% and 23% of the reviewed articles, respectively. Such a condition was the norm when addressing APTs, which dealt with incomplete information and uncertain game states in an adversarial situation.

Moreover, this trend was also followed by Markov and signaling game processes, which accounted for about 25% of the reviewed articles. This situation reflected the trend of research articles incorporating such game processes where specific situations depended on the previous states (decision chains) or triggers (signals) to effectively overcome APTs. Nevertheless, dynamic game types were still a prominent game-theory approach when dealing with APTs since those variations (Bayesian, Markov, signal, and stochastic) were introduced to fit particular security needs and requirements.

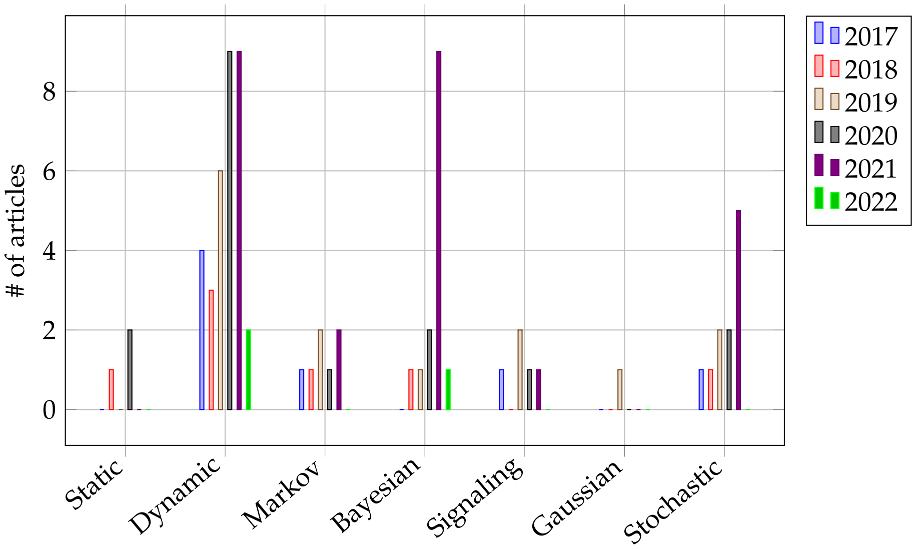

Figure 7. Publication output by year based on the game-theory process type adopted against APTs.

Moreover, several added-values dominated the final 48 articles considered in this review. For instance, concepts, such as bounded rationality, were adopted by several researchers [34,36,57,76,82,86], which imitates the decision-making of agents who have limited rationality and information available in a given adverse situation (both in capacity and time) in order to make satisfactory choices. Furthermore, some studies [36,59,66,76,91] used prospect theory to imitate the actual behaviors of two opposing parties in a variety of application domains. These were among the approaches that considered the practical behaviors of the involved parties when operating with limited information (or uncertainty) and overcoming (or valuating) the risk of aversion.

Another perspective of the study involved deterring adverse situations by being deceptive—called defense deception. Defense deception utilizes several intuitive techniques to mislead attackers. For instance, lying costs were optimized to determine the privacy of partial information (i.e., revealing cues via "cheap-talking") [65,77], thereby, reducing the misalignment between different incentives [65,81], providing an alternative perspective that tilts the information asymmetry (or cognitive bias) [39,86,90,94], encouraging more conservative behaviors instead of aggressive ones [86,94], and discovering novel rules to achieve a better trade-off between security and usability [39,86,90].

Several researchers adopted differential games to sufficiently describe and analyze the dynamic process of adversarial conditions (i.e., attack versus defense). This condition is particularly critical when operating with incomplete information since capturing the system information is complex and may cause many uncertain factors that result in random changes to the system state or strategy [61,66,87].

Some researchers described it as a state-evolution model [66,70], where random factors influence and change in intensity [87]. Differential games also rely on the optimal control principles to attract either the global [70,80] or the saddle-point [87] of the system equilibrium. Typically, control and payoff functions are integrated to describe the algorithmic selection of real-time responses [87], particularly when associated with shifting resource vulnerabilities on a variety of attack surfaces (c.f., moving target defense with different spatial dimensions and informational elements [88]).

Huang et al. [61] constructed a multi-stage and multi-state Markov differential game model to analyze real-time attack–defense behaviors and resolve the persistent defense decision-making challenge by calculating the strategy control function over time, thus, allowing for a more guiding role in the timeliness of the decision-making. Furthermore, a differential dynamical system was introduced to protect cloud storage systems [66] and enterprise group systems [80] while mitigating loss and capturing the time-variance in confrontations between the attackers and defenders.

Moreover, Yang et al. [64] and Yang et al. [70] modeled an APT repair problem as a differential Nash-equilibrium game (the attacker attempted to maximize the potential benefits, while the defender mitigated the potential losses) using an epidemic model based on three practical situations: time-varying communication, the lateral movements of APTs, and the changes of attack–repair strategies over time. Subsequently, the key to solving a differential game was deriving the optimal system by using the associated Hamiltonian principles and determining the Nash equilibrium conditions for the game [79,80].

It is worth noting that, among the adopted game-theory approaches for the defense and detection against APTs, AI techniques were among the scarcely adopted techniques, even in recent years. Only two of the 48 final articles reviewed adopted AI techniques to address specific sub-problems of the game-theory approaches. For example, Laszka et al. [62] adopted a simulated annealing algorithm to find a near-optimal detector configuration to mitigate the attackers' action in an intelligent traffic control game model.

Li et al. [95] incorporated a deep reinforcement-learning technique based on convolutional neural networks and information-rich features to proactively addresses APTs. Nevertheless, both AI techniques require data availability and were applied for a very narrow scope of their respective uses, which can be counter-intuitive against the APT scenario. As game theory provides a framework capable of proactive defense and detecting uncertainty caused by APT [39], AI technique integration with game theory could potentially enhance the system's capability while mitigating adverse conditions, thus, providing a fertile topic for future investigation.

4.2.2. Challenges and Benefits of Adopting Game-Theory Approaches in APT Detection and Prevention

The challenges of game-theory approaches for addressing APTs are summarized in Table 7. The major challenge found among the considered articles was the asymmetricity of the informational structure between an attacker and a defender. Such a situation allowed for risk or uncertainty to be managed and modeled as probability distributions instead of real-value payoffs [73,92]. Such asymmetricity could also be dependent upon the types of devices [32], the types of attacker influence [59,60], and the dynamic interactions between different stages or phases of a modeled game structure [38,73,89]. However, this asymmetric information focused on the context of the detection, which was related to the weighting or the valuation of compromising those informational structures, which is typically costly at the operational and tactical levels of an organization.

Table 7. Summary of the challenges of game-theory approaches against APTs based on the research articles.

References	Challenge Criteria
Xiao et al. [91]; Abass et al. [93]; Rass et al. [57]; Xiao et al. [59]; Min et al. [60]; Lee et al. [26]; Huang et al. [61]; Wang et al. [67]; Horák et al. [68]; Moothedath et al. [69]; Gill et al. [40]; Tan et al. [75]; Tian et al. [76]; Yang et al. [79]; Huang and Zhu [81]; Merlevede et al. [83]; Tan et al. [88]; Halabi et al. [56];	Cost Offshoot
Rass et al. [92]; Chen and Zhu [32]; Xiao et al. [59]; Min et al. [60]; Zhu and Rass [38]; Lv et al. [63]; Yang et al. [64]; Pawlick et al. [33]; Pawlick et al. [65]; Li and Yang [66]; Wang et al. [67]; Horák et al. [68]; Huang and Zhu [39]; Moothedath et al. [69]; Yang et al. [70]; Li et al. [71]; Zhang et al. [72]; Zhang and Zhu [73]; Gill et al. [40]; Bakker et al. [74]; Hu et al. [34]; Tan et al. [75]; Tian et al. [76]; Ye et al. [77]; Xie et al. [78]; Gao et al. [80]; Huang and Zhu [81]; Feng et al. [82]; Nisioti et al. [84]; Tian et al. [36]; Joshi et al. [85]; Bakker et al. [86]; Tan et al. [88]; Halabi et al. [56]; Liu et al. [89]; Seo and Kim [90]; Wan et al. [94]; Li et al. [95];	Asymmetricity
Rass et al. [57]; Pawlick and Zhu [58]; Huang et al. [61]; Laszka et al. [62]; Pawlick et al. [65]; Huang and Zhu [39]; Moothedath et al. [69]; Li et al. [71]; Hu et al. [34]; Yang et al. [79]; Joshi et al. [85]; Mi et al. [87]; Halabi et al. [56]; Liu et al. [89]; Wan et al. [94]; Li et al. [95];	Sensitivity
Xiao et al. [91]; Pawlick and Zhu [58]; Lee et al. [26]; Huang et al. [61]; Lv et al. [63]; Pawlick et al. [33]; Li and Yang [66]; Yang et al. [70]; Bakker et al. [74]; Hu et al. [34]; Tan et al. [75]; Tian et al. [76]; Ye et al. [77]; Gao et al. [80]; Feng et al. [82]; Merlevede et al. [83]; Nisioti et al. [84]; Mi et al. [87]; Tan et al. [88]; Liu et al. [89]; Li et al. [95];	Micro-management

Another challenge to asymmetricity in informational structures that is also influential in the context of defense against APTs was generally identified as defense deception. Such situations involved the fusion of different data sources [63,75,84,94]; the withholding of specifics about data (differential privacy) [77]; delay tactics by repairing [64]; a multi-level interdependent mechanism that validates/justifies another [33,34,71,84,94]; the exposure of a potential perpetrator by leaking some evidence [65] or a stage-wise judicial decision [39,81]; the restriction of resources to starve a potential threat [72]; and the corroboration of interaction levels with other factors [76,80,85,95]. These defense-deception mechanisms demonstrated the level of complexity involved in defending against APTs, where the disadvantages of the attackers in the form of missing or incomplete information are used for the defender's advantage via passive [63,65,75,77,84,94] or proactive responses [33,34,39,64,71,72,76,80,81,84,85,94,95].

Furthermore, other studies addressed the challenge of asymmetricity in the informational structures by focusing on optimal defense strategies that mirrored the attackers [56,67,78,80]; characterizing the best response [34,72,85,86,88]; delaying the attackers by employing a honeypot (decoy mechanism) [36,68,76,81,90]; managing the expected loss through dynamic recovery [66,70] or cyber-insurance [82]; tagging data to identify suspicious information flows [69]; characterizing the signature or profile of the attack [40,75,78]; and managing misconceptions (i.e., suspicions of a nonexistent attack) [74,90].

This challenge involved subjective aspects of the threat, where both the defender and attacker could adopt progressive, aggressive, or conservative strategies, depending on the real-time situation at various stages of the game model. Such modeling has successfully defended against APTs but requires careful consideration of the trade-offs between practicality and performance, particularly when mitigating insider threats (where they could access privileged information for financial gain) [66].

Other challenges that consider the trade-offs between the two metrics were cost offshoot and micro-management, where unexpected or compounding effects of the latter were caused by the former. In contrast, the latter influenced the affinity of the former. For example, the attacker's cost overestimation could be the reason for such a condition due to the defender's uncertain scanning intervals [91,93] or balancing defense decision-making against the state randomness of system security [61]. Furthermore, the defender could also vary its strategies (i.e., periodic strategy) and estimate the compromise probability based on control incentives [58].

Another condition was the integration of security vulnerability quantification, involving an attack tree, the common vulnerability scoring system (CVSS), and game-theory approaches to provide objective evaluations while anticipating and preparing countermeasures against an adversary [26]. In addition to complementing the limitations of the approaches, managing them requires specific calibrations relative to the identified vulnerability to avoid the over-fitting of anticipated countermeasures, which could lead to a predictable routine.

Other challenges were related to the adoption of a periodic strategy, where the time between consecutive moves in the game-theory model was constant; therefore, the player "utility" of the game (attacker or defender) relies on the gains and costs of the available resources over time, which requires characterizing and anticipating optimal strategies to fend off the threat [83]. In contrast, random disturbances and stochastic times between consecutive moves in the game-theory model require maximizing the defense effectiveness and minimizing the cost.

This situation required efficient management that could be sensitive to any perturbation [61,87]. Another aspect of the sensitivity that is challenging when related to APTs is choosing an optimal defense strategy when the strategy space is massive and computationally exhaustive due to the sheer number of interactive elements within the system (i.e., the IoT, transportation, and network node security) [62,79,94,95]. Such a situation is similar to the cost-offshoot challenge and could further perpetuate the APT detection and defense complexity.

In contrast, several benefits have been gained by adopting game-theory approaches for addressing APTs as summarized in Table 8. One major benefit gained from game-theory approaches was through their stability and reliability in the intended system, where the defense performance could be efficiently determined [26,38,87] while capturing the essence of the coordinated attacks [57] and providing locally asymptotically stable points of the game states [87,93].

Furthermore, the timeliness of decision-making and the scope of the application were improved by Huang et al. [61] through the application of the Markov decision-making method in a continuous multi-dimensional phase space with problem variations while considering payoff discounting. Furthermore, Zhu and Rass [38] offered a reasoning approach that systematized the whole system based on local security assessments and defined scores that could be tailored to specific contexts, leading to enhanced timeliness and a substantial increase in reliability.

In another study, decision probability played a crucial role in addressing an APT, as the computational performance was advantageous when the size of the strategy space was computationally expensive [62], the decisions were multi-layered [65], and random disturbances were considered [87]. In other words, it was advantageous to identify and determine the best strategies to overcome the threat before it occurred [61,62].

Table 8. Summary of the benefits of game-theory approaches against APTs based on the research articles.

References	Beneficial Criteria
Xiao et al. [91]; Rass et al. [57]; Chen and Zhu [32]; Xiao et al. [59]; Min et al. [60]; Yang et al. [64]; Li and Yang [66]; Huang and Zhu [39]; Li et al. [71]; Zhang et al. [72]; Zhang and Zhu [73]; Gill et al. [40]; Ye et al. [77]; Xie et al. [78]; Gao et al. [80]; Huang and Zhu [81]; Joshi et al. [85]; Bakker et al. [86]; Halabi et al. [56]; Liu et al. [89];	Utility Changes
Rass et al. [92]; Pawlick and Zhu [58]; Laszka et al. [62]; Pawlick et al. [65]; Wang et al. [67]; Horák et al. [68]; Huang and Zhu [39]; Yang et al. [70]; Li et al. [71]; Bakker et al. [74]; Tian et al. [76]; Ye et al. [77]; Xie et al. [78]; Yang et al. [79]; Huang and Zhu [81]; Feng et al. [82]; Merlevede et al. [83]; Nisioti et al. [84]; Bakker et al. [86]; Mi et al. [87]; Tan et al. [88]; Liu et al. [89]; Wan et al. [94]; Li et al. [95];	Decision Probability
Abass et al. [93]; Rass et al. [57]; Lee et al. [26]; Huang et al. [61]; Zhu and Rass [38]; Laszka et al. [62]; Lv et al. [63]; Yang et al. [64]; Pawlick et al. [33]; Pawlick et al. [65]; Li and Yang [66]; Wang et al. [67]; Horák et al. [68]; Moothedath et al. [69]; Li et al. [71]; Zhang et al. [72]; Zhang and Zhu [73]; Gill et al. [40]; Hu et al. [34]; Tan et al. [75]; Tian et al. [76]; Ye et al. [77]; Yang et al. [79]; Feng et al. [82]; Merlevede et al. [83]; Nisioti et al. [84]; Tian et al. [36]; Joshi et al. [85]; Mi et al. [87]; Tan et al. [88]; Halabi et al. [56]; Liu et al. [89]; Seo and Kim [90]; Wan et al. [94]; Li et al. [95];	Stability/Reliability
Rass et al. [92]; Chen and Zhu [32]; Lee et al. [26]; Zhu and Rass [38]; Yang et al. [64]; Pawlick et al. [33]; Wang et al. [67]; Huang and Zhu [39]; Moothedath et al. [69]; Yang et al. [70]; Gill et al. [40]; Bakker et al. [74]; Hu et al. [34]; Tan et al. [75]; Tian et al. [76]; Xie et al. [78]; Yang et al. [79]; Nisioti et al. [84]; Tian et al. [36]; Joshi et al. [85]; Mi et al. [87]; Tan et al. [88]; Seo and Kim [90];	Objective Assessment
Zhu and Rass [38]; Lv et al. [63]; Yang et al. [64]; Horák et al. [68]; Huang and Zhu [39]; Moothedath et al. [69]; Zhang and Zhu [73]; Bakker et al. [74]; Hu et al. [34]; Tan et al. [75]; Gao et al. [80]; Bakker et al. [86]; Tan et al. [88]; Halabi et al. [56]; Seo and Kim [90]; Wan et al. [94]; Li et al. [95];	General Pattern

The general pattern of detecting a malicious entity can be to fuse data from different sources to compute a comprehensive payoff and optimally allocate constrained secure resources [63], allocate the available repair (or recovery) resources to mitigate potential losses [64,79], predict risk compensation via the effect of insurance [73,82], select suitable defense timing [56,75,76,88], tag sensitive information flows [69], or actively expose vulnerabilities (e.g., a honeypot) [36] while conducting an objective assessment on the expected state of the target system [33,40,64,66,75,79].

An interdependent model of trust management decisions that involve multi-layered optimization provided structural reliability when multiple or dynamic games were considered to cater to the diverse possibilities of APTs [33] and did not always strive to eliminate leakage when deception cues could be used as deterrents [65]. In Hu et al. [34], they introduced a more generalized approach that involved different social players by measuring and quantifying their rational degrees and simulating their growth to reflect the randomness and inertia of the population's social behaviors for realistic attackers and defenders.

In Seo and Kim [90], they investigated a defender-deception method (e.g., honeypot and decoy that induced cognitive bias and induction) that were formulated for the scenario and attributed to the secure dominant organizational share, and they presented an optimal strategy that minimized the performance degradation and maximized their efficiency while constructing a deceptive container-management plan that yielded the highest defense and the lowest cost for defenders with limited utilities.

Another approach to decision probability incorporated novel metrics to improve the benefits of being reliable and objective in APT defense. For instance, Wang et al. [67] introduced the concept of defense effectiveness that quantified the impact of a defense strategy against an attack strategy when both sides had reached a balanced state, which was based on the prior belief and payoff of the defender when selecting the optimal defense strategy. Another study by Horák et al. [68] modeled the uncertainty of the defender using beliefs that mapped onto the probability distribution over the subsets of the possible security states.

In Zhang et al. [72], they provided a response characterization in more general settings where the challenges faced by the defender and attacker were a continuous convex optimization and a fractional-knapsack problem, respectively, resulting in an effortless determination of the response strategy. These conditions were also applicable when resources were limited [67,68,72]. Furthermore, Ye et al. [77] adopted differential privacy techniques that preserved the privacy of the systems in networks, mitigating utility gains of the attackers while retaining the system performance under various conditions.

Some studies focused on the benefits of reliability and stability while providing good frameworks for decision probability when addressing APTs. For example, Merlevede et al. [83] assumed the strategies chosen by both sides (attacker and defender) were from restricted strategy spaces and between exponential and periodic strategies, which was practical for the incentive design for time-based security decisions. Furthermore, Nisioti et al. [84] proposed a Bayesian Cyber-Investigation Game (BCIG) that assumed a probabilistic distribution calculated from past incident reports and adopted an anti-forensic technique on the side of the defender to increase the collected benefits across a wide range of investigations while decreasing the costs.

Furthermore, a multidimensional transition of attack and detection surfaces was analyzed by Tan et al. [88] and Wan et al. [94], where the characteristics of stealth interactions (stochastic, aggressive, and conservative) were represented, thus, allowing for a generalized and objective view of the trends in the state transitions of a network system. In addition, Liu et al. [89] quantitatively analyzed the safety in cyber–physical interactions using a weighted, colored Petri net and attack models that calculated the attack weights by using a threat-propagation matrix as well as a security-state vector. Explainability was also integrated into dynamic and persistent risk-assessment schemes with resource-allocation mechanisms [95]. Security awareness could also significantly accelerate security monitoring, analysis, and comprehension.

Another benefit was found via utility change, such as the competitive strategy profile proposed by Li and Yang [66], where the necessity system guided the defender to search for an admissible set of strategies and randomly outperform the generated strategy profiles. This situation allowed for the dynamic recovery strategy to be competitive and practical when compared to relying on the dynamic attack strategy alone. Furthermore, in a one-shot game model (where interactions only happened once), a trigger strategy (choosing a certain strategy at the beginning and adapting later) was adopted to address the main priority of the target system (maximize defenses or mitigate losses) [71], or the strategy incorporated bounded rationality to influence the attacker's appraisal [36,76].

In a system of centralized or distributed connectivity of the defenders (i.e., IoT devices and fog computing), the optimal incentive-compatible insurance contract insured half of the defender's losses, which were quantitatively determined by the loss parameters of the device ownership [73], and cyber-insurance-enabled security provided service coverage [82]. Such conditions have allowed for an acceptable level of economic/financial losses [40,73,82].

However, a study by Halabi et al. [56] focused on integrating a new layer of robustness in the defense architecture designed to increase its tolerance of sophisticated attacks resulting from APTs. Furthermore, an insider threat's advantage in assisting APTs could be deterred or mitigated by optimizing the initial defensive mechanism via modeling the organizational culture (i.e., limiting the information that a defender could have and diversifying its utility functions) [85].

4.2.3. Implications and Converging Topics for Future Work in Defense and Detection against APTs

As the trends of APT detection and prevention have converged with game-theory approaches, several implications were observed. These implications included optimized protective performance, a full-fledged simulation tool for security scenarios, a security-as-service paradigm, a form of trust framework, the prioritization of repair over protective details, the conversion of deception into protection, and the encouragement of richer quality interactions between the attacker and the defender.

Several studies focused on optimizing the protective performance of a game-theory approach against APTs. In one study, the cloud storage system's data protection level and the defender utility were improved by learning faster and being more resistant to APT attackers who chose an attack policy based on the estimated defense learning scheme [60]. In another article, a game-theory-based vulnerability quantification method allowed for the objective calculation of the security vulnerabilities of a network system (e.g., social IoTs [26] or moving-target defense (MTD) [75,88]) while anticipating and preparing for countermeasures against adversarial attacks [26,34,38].

A differential game model was developed to analyze dynamic, continuous, and real-time attack–defense processes to predict a multi-stage continuous attack–defense process [61,67]. Repeated defense actions were used for employee awareness training based on information gathered from APT incidents and enhanced model flexibility [38]. Some studies investigated the spatiotemporal aspects of an attack [75,88], making this an essential addition to the attack-surface transformation process.

Game theory and the consideration of time-evolved states [70] and Bayesian game theory to infer incomplete information regarding an attacker's behaviors was used to determine optimal defense strategies [89]. These approaches provided a more comprehensive, dynamic, and practical approach to addressing APT attacks.

Some studies encouraged a game-theory approach as a simulation tool for recreating the security scenario with subjective attacking behaviors [57,91]. Such a perspective allowed for evaluating optimal risk mitigation strategies based on the available information while easily addressing adversary modeling issues [36,91]. This condition was particularly useful in defending against APTs because uncertainty exists in the attacker's capabilities, incentives, and induced damages.

Using matrix games with distributed payoffs, where the game is in discrete time for one player but continuous time for the other, has allowed for the natural mitigation of APTs [57,92]. In addition, a physical understanding of the infrastructure and theoretical methods can be combined to create a practical solution; define appropriate model parameters, proper categories, and representative definitions; and design suitable payoff modeling [57]. Due to the probability-weighting distortion, a subjective attacker tends to overestimate the attack cost and, thus, attacks less frequently in cumulative prospect theory (CPT)-based detection games, thus, improving the data protection and cloud utility [59].

Furthermore, the existence of Bayesian–Nash equilibrium strategies has been proven under bounded rationality. At the same time, changing the strategy selection and utility, improving the detection rate, and increasing the comprehension of adversarial behaviors in a grid system [76] and the IoT [36] have also been addressed.

Using the security-as-service paradigm, the best contract design was investigated for a cloud-enabled internet of controlled things (IoCT). Optimal contract design was determined based on cloud security quality, where payoff compatibility and contract penalty was utilized, alongside the payoff of the cloud service providers when optimizing the security utility [32].

In one study, a game-theory approach based on the FlipIn framework was adopted to design incentive-compatible, welfare-maximizing cyber-insurance contracts, and this offered a theoretical foundation for the quantitative assessment of cyber-risks, the development of cross-layer defense mechanisms, the design of cyber-insurance policies [73], and the development of the pricing problem as an optimal control problem via a hierarchical dynamic game framework [82].

Moreover, a game-theory model of cyber attacks on traffic control was introduced to provide a theoretical foundation for planning and improving the performance of delivered services, as well as for implementing countermeasures against the risks posed by cyber attacks on transportation networks and infrastructures (e.g., traffic signal tampering [62] and the internet of vehicles [56]).

A unique take on countering APTs was provided in the form of a trust framework, where vulnerabilities and risks were passively identified by integrating a trustful system or a set of procedures as part of the game-theory elements. A framework of trust built on incentives and costs for system control was incorporated. This allowed for continuous decision-making, a better understanding of strategic trust, and multi-layer security [33,58]. In addition, such a framework improved the level of data protection and had a faster learning speed for strategic defense selection [95].

A combination of different data sources (e.g., network protocols and log documents) was used to precisely calculate the payoff of a game-theory approach. This situation allowed the Nash equilibrium to be computed in order to detect the possibility of a malicious attack while maintaining the target system functions and providing effective protection [63]. Another approach via differential privacy was designed to resist attacks regardless of the attackers' rationale and to increase the complexity of attack formulations, thereby, giving administrators more time to build defense policies [77].

An effective dynamic-recovery (DR) strategy to mitigate the total loss of a cloud defender in the face of an APT campaign was investigated by Li and Yang [66]. The concept introduced a competitive strategy profile that outperformed other randomly generated strategies and enhanced the APT defense capabilities [69] particularly in situations where insiders with privileged access could facilitate the APT campaign for financial gain [81]. Moreover, an organization subjected to APT could flexibly divide a long repair time into several relatively shorter repair periods.

The corresponding potential repair strategy in this time horizon was realized by estimating its expected state. Although the APT repair game was open-loop and lacked flexibility, the organization could handle the APT in a closed-loop manner for the most part and mitigate its potential loss even further [64]. Another study by Yang et al. [79] formulated a model based on a data backup-and-recovery system (DBARS) when defending against APTs by proactively seeking out and eliminating the compromised portion of a system via evolution, leading to a potentially cost-effective real-time solution [69].

Many studies focused on making deception an advantageous situation for the protector. However, the techniques for detecting deception in cybersecurity should not always aim to eliminate leakage, as revealing specific cues to deception could serve as a deterrent [65]. Such a condition could be used to design the detection mechanisms for implementing online policies without requiring iterative numerical computations. In some situations, game representation and algorithmic design encumbered the scalability of the solution [68] and its interoperability [40]. Legitimate system users could also be compromised.

The use of defensive deception could also generate uncertainties for attackers and motivate them to take more conservative behaviors [39]. A belief concept was introduced as a proactive defensive response to provide a probabilistic detection system, achieve a better payoff rate, and prevent effectual reconnaissance. However, the strict resources could characterize their behavior as an adaptive strategy instead [72]. Moreover, a hypergame was proposed as a valuable model to analyze the effects of adversarial perturbations and stochastic conditions to better understand cyber attackers and defenders in control systems [74,86].

The concepts of the motive and deterrence thresholds were introduced to assess the average motive of the insider population and the adequacy of the honeypots [81,85]. Considering the incomplete and deceptive nature of the organizational environment and information vulnerability, researchers constructed proactive deception strategies based on the organizational domain and simulated their related improvements in deception efficiency, which was intended to minimize performance degradation and maximize security [90].

Finally, richer quality interactions between the attacker and the defender have been realized in several studies. The real-world interactions between cyber attackers and defenders were realistically modeled to predict the differences in their behaviors, strategies, and tactics under various conditions [71,78]. In some cases, the computational overhead increased, which demanded a higher observation cost of vulnerable resources [78]. Increasing the paralysis threshold (the point at which a group cannot continue interacting) within a specific range could facilitate a short-term, high-intensity interaction.

In addition, effective strategies should be implemented as early as possible to achieve dominance and affect the network states. This condition suggested that obtaining an equilibrium strategy was challenging when interaction strategies were mutually restrictive [80]. The research emphasized the importance of considering the timing of security decisions (exponential and periodic) and the impact of the passing of time on the valuation of a resource in security policy-making, where an attack could be disincentivized and information symmetry overcome between the attacker and the defender [83].

The importance of using anti-forensic techniques was emphasized in a forensic investigation of real-world scenarios, which considered additional parameters, assumed multiple attacker types at each decision point, and combined other optimization methods [84]. Another aspect presented by Mi et al. [87] provided a reference for selecting an optimal defense strategy (or increasing it beyond the limit) while ensuring its advantage, maximizing defense effectiveness at a minimum cost, and minimizing loss when the defense was not possible. Moreover, mitigation of the uncertainty perceived by both the attacker and the defender led to higher resilience and high expected utility [94].

From the identified implications of game-theory applications for combating cybersecurity threats, several converging topics against APTs were noted and summarized as follows:

- Improving the protective performance of a game-theory approach through methods, such as learning faster and being more resistant to attacks; quantifying vulnerabilities; and anticipating and/or preparing for countermeasures.
- Analyzing dynamic, continuous, and real-time attack–defense processes to predict multi-stage continuous attack–defense processes and improve awareness of future attacks (i.e., employee training).
- Using game theory as a simulation tool to recreate security scenarios with subjective attacking behaviors that are practical and realistic, consider spatiotemporal aspects of attacks, infer incomplete information about attacker behavior, and evaluate optimal risk mitigation and defense strategies.
- Investigating optimal contract design, designing incentive-compatible and welfare-maximizing cyber-insurance contracts, and formulating the pricing problem as an optimal control problem through a hierarchical dynamic game framework.
- Applying game theory by optimizing the security of cyber–physical systems (CPS) and transportation systems by considering various factors, such as the attacker behavior, system constraints, and the interdependence of components.
- Using game theory to optimize the security of social networks by considering the influence of users on each other’s behaviors and the strategic interaction between users and a network administrator.

As one of the most pervasive information and communication technologies, the use of smartphones over the last decade has increased dramatically. As a result, smartphone usage has faced threats at all stages of application utility, from application downloads being implanted with malicious codes, application installation or usage that contains malicious programs, and even uninstalled applications that leave behind malicious residual code [97]. In addition, a plethora of features exist in smartphones, such as inertial sensors, positioning sensors, ambient sensors, telephony services, telecommunications, and other utilities, that provide a continuous flow of information and an accurate description of a user’s routines and behaviors, thereby, enabling an attacker to generate a highly specific and successful APT campaign [4].

As such, smartphone security is a critical topic that requires the attention of academia and industry alike. In general, mobile APTs are defined as sophisticated attacks in mobile-device environments where social engineering has been used to leak data using features that are innate for information management (e.g., sensors and services). However, the threat in mobile devices is still nascent and challenging to assess, as identifying an attacker is difficult due to the following reasons [2]: (i) high accessibility; (ii) various initial points of access; and (iii) jurisdictional limitations that are relatively low-entry and high-reward. As such, there is a significant possibility that a broader diversity of attacker avatars exist, from nation-state bad actors motivated by national interests to savvy individuals focused on personal gain.

In addition, attack procedures associated with the established threat actors in the mobile environment were also related to threat actors in the PC environment [9]. This condition allowed threat actors to move freely between PC and mobile environments to achieve their goals. Therefore, it is possible to improve the understanding of the current cyber-threat environment using traditional cyber-attribution methods that employ complex evaluations of both their technical and socio-political attributes [2,9]. Furthermore, since mobile APTs can originate from diverse regions and borders in different countries and regulations, jurisdictional limitations can hinder cross-border cyber-crime investigations while preventing the progress of collecting evidence. However, the rapid growth of mobile devices in various fields where massive volumes of data are constantly generated could take advantage of the converging topics on game-theory approaches as a suitable solution for addressing mobile APTs.

However, public datasets and data on mobile-based APTs are scarce, which may impede research progress regarding the detection of and defense against new generations of APT attacks (e.g., using mobile, IoTs, and other smart devices). Recent solutions have involved the adoption of the situational-awareness (SA) model, also known as the observe–orient–decide–act (OODA) framework, which mitigates APTs by conceptually monitoring the fingerprinting of mobile device behaviors [16].

Regarding another aspect, Al-Kadhimi et al. [98] provided a solution to improve the awareness of APT detection on smartphones based on the correlation of the MITRE Framework and an attack tree, called a fingerprint, for a mobile-sensor APT-detection framework (FORMAP). Similarly, Jabar et al. [99] proposed a framework for mobile APT detection based on device behavior (SHOVEL), and this study demonstrated the impacts of APT attacks on user behavior when self-adaptive, auto-predictive, and auto-reflective considerations were present in their decision-making. As such, this direction could be ideal for future game-theory-based research endeavors.

5. Limitations and Future Outlooks

Although the trends, benefits, challenges, and implications of the game-theory approaches against APTs were characterized, there are certain limitations in the current review. First, one study limitation was related to the small research team and the associated time restrictions. As such, the study could not evaluate all possible coverage, perspectives, and potential trends concerning this topic. Instead, the general concept and the majority of the considered literature represent the current knowledge of the topic. Another limitation of this study was our focus on game-theory approaches related to APT detection and prevention. However, other aspects of APTs could also be considered (i.e., vulnerability, risks, aftermath, awareness, and preventive measures). Other aspects that could be overlooked when using game theory to address APT attacks include:

- Human factors: Game-theory models generally assume that the actors (e.g., attackers and defenders) are rational and make decisions based on a clear set of objectives and preferences [77]. However, in real-world situations, human behavior can be influenced

by various factors, such as emotions, biases, and social pressure, which game-theory models may not capture [85].
- Legal and ethical considerations: Game-theory models often involve trade-offs between different objectives, such as security and privacy, or between stakeholders, such as users and service providers. These trade-offs may have legal or ethical implications that must be carefully considered.
- Practicality and limited flexibility: Game-theory models may only be practical or feasible to implement in real-world situations under specific circumstances, particularly if they require significant resources or involve complex or expensive technologies [77]. Game-theory models are generally designed to analyze specific security scenarios or behaviors. If the threat environment changes or new types of attacks emerge, it may be necessary to develop new models or modify existing ones to address these changes. This can be a time-consuming and resource-intensive process.
- Misuse or misappropriation: Game-theory models may be misused or misunderstood by practitioners who lack a thorough understanding of their limitations and assumptions. This situation can lead to inappropriate or ineffective security measures being implemented.
- Interactions with other approaches: There may need to be more than game-theory models involved to comprehensively address APT attacks. They may need to be combined with other approaches, such as risk assessment, vulnerability management, and incident response. Therefore, it is essential to consider how game-theory models fit into a security strategy and the interactions between different approaches.
- Complexity and data requirements: Game-theory models can be complex and may require significant mathematical and analytical skills to understand and apply. This can make it difficult for practitioners with limited technical expertise to use game theory effectively. Game-theory models often require extensive data about the behavior of attackers and defenders and the costs and consequences of different actions. In cases where such data are unavailable or unreliable, it may be difficult to use game theory effectively.
- Assumptions and limited applicability: Game-theory models are based on certain assumptions about the behavior and motivations of attackers and defenders. If these assumptions are invalid, the model's results may not be accurate or applicable to real-world situations. Game theory may not be suitable for addressing certain APT attacks or security scenarios. For example, game theory may not be effective in situations where the motivations or objectives of the attackers are not clearly defined or are difficult to anticipate.

It is challenging to predict future developments in the use of game theory to address APTs, as it depends on many factors, such as advances in technology, changes in the threat landscape, and the emergence of new trends in security research. However, current evidence has shown that game theory can continue to be a valuable tool for addressing APT attacks, as it provides a framework for analyzing and understanding the strategic interactions between attackers and defenders and can be used to optimize the security of various types of systems. Some potential areas of future research that involve the use of game theory to address APT attacks include:

- Developing more sophisticated game-theory models that can better capture the complexity and uncertainty of real-world security scenarios, including the potential for multiple attackers and defenders with different motivations, capabilities, and resources.
- Incorporating machine-learning techniques into game-theory models to enable the more accurate prediction and optimization of security outcomes and to adapt to changing threat environments and evolving attacker behaviors.
- Applying game theory to emerging technologies, such as quantum computing, blockchain, and artificial intelligence, may present new challenges and opportunities for APT attacks and defenses.

- Investigating the use of game theory to optimize the security of emerging technologies, such as smartphones, fog and edge computing, the internet of things (IoT), smart cities, and related critical infrastructure systems (e.g., energy, healthcare, finance, law enforcement, and the government) that may be particularly vulnerable to APT attacks.
- Developing game-theory approaches for managing and mitigating the impacts of APT attacks, including methods for minimizing damage, recovering from attacks, and preventing future attacks.

Governments could also take real-world actions, alongside lawmakers and other organizations, to address APTs, such as by developing and implementing effective cybersecurity policies and regulations to establish minimum security standards for organizations and individuals and provide guidance for APT protection. Several governments and related organizations should also invest in research and development to better understand APT attacks and develop new technologies and techniques for defending against them.

Moreover, cybersecurity awareness and education programs should be promoted to help individuals and organizations understand the risks associated with APT attacks and methods to protect against them. In addition, creating a channel for private sectors and strengthening international cooperation should be conducted to disseminate information about APT attacks and develop coordinated responses to potential threats while forming international agreements and frameworks to prevent and mitigate APTs. Finally, effective incident response capabilities should be developed and maintained to respond quickly and efficiently to APTs and other cyber-related incidents.

6. Conclusions

Based on this literature review, a plethora of studies have applied game theory as a tool for addressing APT attacks. Game theory provides a framework for analyzing and understanding the strategic interactions between attackers and defenders. It has been used to optimize the protective performance of security measures, anticipate and prepare for countermeasures, and design incentive-compatible and welfare-maximizing contracts. Game theory has also been applied to optimize the security of cyber–physical systems, social networks, and transportation systems, among others. Game theory will continue to be a valuable tool in addressing APT attacks in the future. It provides a means for analyzing and understanding complex security scenarios and can be used to optimize the security of various types of systems.

It is difficult to predict the trends of APTs in the future, as this will depend on many factors, such as technological advances, changes in the threat landscape, and the emergence of new trends in cyber-crime. However, APT attacks are likely to continue to evolve and become more sophisticated, thus, posing significant challenges for defenders and requiring ongoing efforts to outpace emerging threats. Some potential trends that may emerge include the use of automation, where APT attacks become more automated and sophisticated, and attackers using tools and techniques, such as machine learning and artificial intelligence, to automate various aspects of the attack process. This situation could make it more difficult for defenders to detect and respond to attacks.

In addition, attackers may focus more on emerging technologies, such as quantum computing, block-chain, and the internet of things (IoT), which may be exploited as a medium or as actors for different stages of an APT. This situation may present new opportunities and challenges for APT detection and prevention. Moreover, APT attackers are likely to continue evolving their tactics and techniques to bypass defenses and evade detection. This condition may include the use of new types of malware, the exploitation of new vulnerabilities, and the use of more sophisticated social-engineering techniques. This situation may also lead to more targeted APTs that focus on specific industries and sectors of particular interest or value (e.g., healthcare, finance, critical infrastructure, and the government).

Funding: This work is supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme with project Code: FRGS/1/2020/ICT07/USM/02/2. This work is also part of the project supported by the International Research Center for AI and Entertainment Science, Japan Advanced Institute of Science and Technology.

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

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A. Extraction Form

Table A1 is the extraction form used for extracting the information of the reviewed articles.

Table A1. Extraction form used for the detection and defense of APT studies.

Data to Be Extracted	Reviewer Notes
Title of publication Journal Journal domain Author(s) Author location (country and institution) Year of publication Industry application	
M: Objective of the study M: Research methods M: Sources of data M: Research instruments M: Data analysis methods	
V: Model or factors for defense/detection of APT V: Strategies, responses, and features of APT V: Benefits and challenges of APT	
R: Main findings R: Implications R: Conclusions	

M–methodology; V–studied focuses; and R–results.

References

1. Press, L. Personal Computing: The Post-PC Era. *Commun. ACM* **1999**, *42*, 21–24. [CrossRef]
2. Kim, K.; Shin, Y.; Lee, J.; Lee, K. Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator. *Sensors* **2021**, *21*, 6522. [PubMed]
3. Gonzalez-Manzano, L.; Mahbub, U.; de Fuentes, J.M.; Chellappa, R. Impact of injection attacks on sensor-based continuous authentication for smartphones. *Comput. Commun.* **2020**, *163*, 150–161. [CrossRef]
4. Zulkefli, Z.; Singh, M.M. Sentient-based access control model: A mitigation technique for advanced persistent threats in smartphones. *J. Inf. Secur. Appl.* **2020**, *51*, 102431. [CrossRef]
5. Ahmed, Y.; Taufiq, A.; Md Arafatur, R. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Comput. Mater. Contin.* **2021**, *67*, 2497–2513. [CrossRef]
6. Solanas, A.; Patsakis, C.; Conti, M.; Vlachos, I.S.; Ramos, V.; Falcone, F.; Postolache, O.; Pérez-Martínez, P.A.; Di Pietro, R.; Perrea, D.N.; et al. Smart health: A context-aware health paradigm within smart cities. *IEEE Commun. Mag.* **2014**, *52*, 74–81. [CrossRef]
7. Park, M.; Han, J.; Oh, H.; Lee, K. Threat Assessment for Android Environment with Connectivity to IoT Devices from the Perspective of Situational Awareness. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 5121054. [CrossRef]
8. Kumar, R.; Singh, S.; Kela, R. Analyzing Advanced Persistent Threats Using Game Theory: A Critical Literature Review. In Proceedings of the International Conference on Critical Infrastructure Protection, Virtual, 15–16 March 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 45–69.
9. Rass, S.; Zhu, Q. GADAPT: A sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats. In Proceedings of the International Conference on Decision and Game Theory for Security, New York, NY, USA, 2–4 November 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 314–326.
10. Tankard, C. Advanced persistent threats and how to monitor and deter them. *Netw. Secur.* **2011**, *2011*, 16–19. [CrossRef]
11. Sood, A.K.; Enbody, R.J. Targeted cyberattacks: A superset of advanced persistent threats. *IEEE Secur. Priv.* **2012**, *11*, 54–61.

12. Ullah, F.; Edwards, M.; Ramdhany, R.; Chitchyan, R.; Babar, M.A.; Rashid, A. Data exfiltration: A review of external attack vectors and countermeasures. *J. Netw. Comput. Appl.* **2018**, *101*, 18–54. [CrossRef]
13. Zimba, A.; Chen, H.; Wang, Z.; Chishimba, M. Modeling and detection of the multi-stages of advanced persistent threats attacks based on semi-supervised learning and complex networks characteristics. *Future Gener. Comput. Syst.* **2020**, *106*, 501–517. [CrossRef]
14. Steffens, T. Advanced Persistent Threats. In *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–21. [CrossRef]
15. Xing, K.; Li, A.; Jiang, R.; Jia, Y. A Review of APT Attack Detection Methods and Defense Strategies. In Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, 27–30 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 67–70.
16. Jabar, T.; Mahinderjit Singh, M. Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework. *Sensors* **2022**, *22*, 4662. [CrossRef] [PubMed]
17. Pawlick, J.; Farhang, S.; Zhu, Q. Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats. In Proceedings of the International Conference on Decision and Game Theory for Security, London, UK, 4–5 November 2015; pp. 289–308.
18. Basak, A.; Černỳ, J.; Gutierrez, M.; Curtis, S.; Kamhoua, C.; Jones, D.; Bošanskỳ, B.; Kiekintveld, C. An initial study of targeted personality models in the flipit game. In Proceedings of the GameSec: International Conference on Decision and Game Theory for Security, Seattle, WA, USA, 29–31 October 2018; pp. 623–636.
19. Nash, J. Non-cooperative games. *Ann. Math.* **1951**, *54*, 286–295. [CrossRef]
20. Tatam, M.; Shanmugam, B.; Azam, S.; Kannoorpatti, K. A review of threat modelling approaches for APT-style attacks. *Heliyon* **2021**, *7*, e05969. [CrossRef] [PubMed]
21. Hejase, H.J.; Fayyad-Kazan, H.F.; Moukadem, I. Advanced persistent threats (apt): An awareness review. *J. Econ. Econ. Educ. Res.* **2020**, *21*, 1–8.
22. Stojanović, B.; Hofer-Schmitz, K.; Kleb, U. APT datasets and attack modeling for automated detection methods: A review. *Comput. Secur.* **2020**, *92*, 101734. [CrossRef]
23. Bhat, B.A.; Kumar, R. APT: A buzzword and a reality-A bibliometric review of the literature (2010–2020). In Proceedings of the 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; Seventh Int Conf on Data Science & Systems; 19th Int Conf on Smart City; seventh Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Haikou, China, 20–22 December 2021; pp. 1972–1979.
24. Khaleefa, E.J.; Abdulah, D.A. Concept and difficulties of advanced persistent threats (APT): Survey. *Int. J. Nonlinear Anal. Appl.* **2022**, *13*, 4037–4052.
25. Amr. Kaspersky Security Bulletin 2022. *Statistics* **2022**, *1*, 1–19.
26. Lee, S.; Kim, S.; Choi, K.; Shon, T. Game theory-based security vulnerability quantification for social internet of things. *Future Gener. Comput. Syst.* **2018**, *82*, 752–760. [CrossRef]
27. Ahmad, A.; Webb, J.; Desouza, K.C.; Boorman, J. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Comput. Secur.* **2019**, *86*, 402–418. [CrossRef]
28. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1851–1877. [CrossRef]
29. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
30. Bencsáth, B.; Pék, G.; Buttyán, L.; Felegyhazi, M. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet* **2012**, *4*, 971–1003. [CrossRef]
31. Munro, K. Deconstructing flame: The limitations of traditional defences. *Comput. Fraud Secur.* **2012**, *2012*, 8–11. [CrossRef]
32. Chen, J.; Zhu, Q. Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: A contract design approach. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2736–2750. [CrossRef]
33. Pawlick, J.; Chen, J.; Zhu, Q. ISTRICT: An Interdependent Strategic Trust Mechanism for the Cloud-Enabled Internet of Controlled Things. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1654–1669. [CrossRef]
34. Hu, H.; Liu, Y.; Chen, C.; Zhang, H.; Liu, Y. Optimal decision making approach for cyber security defense using evolutionary game. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 1683–1700. [CrossRef]
35. Massacci, F.; Jaeger, T.; Peisert, S. Solarwinds and the challenges of patching: Can we ever stop dancing with the devil? *IEEE Secur. Priv.* **2021**, *19*, 14–19. [CrossRef]
36. Tian, W.; Du, M.; Ji, X.; Liu, G.; Dai, Y.; Han, Z. Honeypot detection strategy against advanced persistent threats in industrial internet of things: A prospect theoretic game. *IEEE Internet Things J.* **2021**, *8*, 17372–17381. [CrossRef]
37. Kumar, R.; Kela, R.; Singh, S.; Trujillo-Rasua, R. APT attacks on industrial control systems: A tale of three incidents. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100521. [CrossRef]
38. Zhu, Q.; Rass, S. On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats. *IEEE Access* **2018**, *6*, 13958–13971. [CrossRef]
39. Huang, L.; Zhu, Q. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Comput. Secur.* **2020**, *89*, 101660. [CrossRef]

40. Gill, K.S.; Saxena, S.; Sharma, A. GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot. *Comput. Secur.* **2020**, *92*, 101732. [CrossRef]
41. National Institute of Standards and Technology. Guide to Industrial Control Systems (ICS) Security. 2015. Available online: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (accessed on 1 January 2023).
42. Homeland Security Systems Engineering; Development Institute. CAPEC: Common Attack Pattern Enumeration and Classification. 2022. Available online: https://capec.mitre.org/ (accessed on 1 January 2023).
43. Corporation, M. NVD CVSS, Common Vulnerabilities and Exposures. 2011. Available online: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-3402 (accessed on 1 January 2023).
44. MITRE. ATT&CK Threat Database, MITRE ATT&CK. 2022. Available online: https://attack.mitre.org/ (accessed on 1 January 2023).
45. RISI. RISI Online Incident Database. 2015. Available online: https://www.risidata.com/Database (accessed on 1 January 2023).
46. Chukwudi, A.E.; Udoka, E.; Charles, I. Game theory basics and its application in cyber security. *Adv. Wirel. Commun. Netw.* **2017**, *3*, 45–49. [CrossRef]
47. Van Dijk, M.; Juels, A.; Oprea, A.; Rivest, R.L. FlipIt: The game of "stealthy takeover". *J. Cryptol.* **2013**, *26*, 655–713. [CrossRef]
48. Myerson, R.B. *Game Theory: Analysis of Conflict*; Harvard University Press: Cambridge, MA, USA, 1997.
49. Ho, E.; Rajagopalan, A.; Skvortsov, A.; Arulampalam, S.; Piraveenan, M. Game Theory in defence applications: A review. *Sensors* **2022**, *22*, 1032. [CrossRef]
50. 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*, 1–37. [CrossRef]
51. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering. Technical Report, Ver. 2.3*; Keele University: Keele, UK, 2007.
52. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*. [CrossRef]
53. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 43. [CrossRef]
54. Nicolescu, L.; Tudorache, M.T. Human–Computer Interaction in Customer Service: The Experience with AI Chatbots—A Systematic Literature Review. *Electronics* **2022**, *11*, 1579. [CrossRef]
55. Petticrew, M.; Roberts, H. *Systematic Reviews in The Social Sciences: A Practical Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2008.
56. Halabi, T.; Wahab, O.A.; Al Mallah, R.; Zulkernine, M. Protecting the Internet of vehicles against advanced persistent threats: A bayesian Stackelberg game. *IEEE Trans. Reliab.* **2021**, *70*, 970–985. [CrossRef]
57. Rass, S.; Alshawish, A.; Abid, M.A.; Schauer, S.; Zhu, Q.; De Meer, H. Physical intrusion games—optimizing surveillance by simulation and game theory. *IEEE Access* **2017**, *5*, 8394–8407. [CrossRef]
58. Pawlick, J.; Zhu, Q. Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2906–2919. [CrossRef]
59. Xiao, L.; Xu, D.; Mandayam, N.B.; Poor, H.V. Attacker-centric view of a detection game against advanced persistent threats. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2512–2523. [CrossRef]
60. Min, M.; Xiao, L.; Xie, C.; Hajimirsadeghi, M.; Mandayam, N.B. Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach. *IEEE Internet Things J.* **2018**, *5*, 4250–4261. [CrossRef]
61. Huang, S.; Zhang, H.; Wang, J.; Huang, J. Markov differential game for network defense decision-making method. *IEEE Access* **2018**, *6*, 39621–39634. [CrossRef]
62. Laszka, A.; Abbas, W.; Vorobeychik, Y.; Koutsoukos, X. Detection and mitigation of attacks on transportation networks as a multi-stage security game. *Comput. Secur.* **2019**, *87*, 101576. [CrossRef]
63. Lv, K.; Chen, Y.; Hu, C. Dynamic defense strategy against advanced persistent threat under heterogeneous networks. *Inf. Fusion* **2019**, *49*, 216–226. [CrossRef]
64. Yang, L.; Li, P.; Zhang, Y.; Yang, X.; Xiang, Y.; Zhou, W. Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach. *IEEE Trans. Inf. Forensics Secur.* **2019**, 14, 1713–1728. [CrossRef]
65. Pawlick, J.; Colbert, E.; Zhu, Q. Modeling and Analysis of Leaky Deception Using Signaling Games with Evidence. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1871–1886. [CrossRef]
66. Li, P.; Yang, X. On dynamic recovery of cloud storage system under advanced persistent threats. *IEEE Access* **2019**, *7*, 103556–103569. [CrossRef]
67. Wang, Z.; Lu, Y.; Li, X.; Nie, W. Optimal network defense strategy selection based on Markov Bayesian game. *KSII Trans. Internet Inf. Syst. (TIIS)* **2019**, *13*, 5631–5652.
68. Horák, K.; Bošanskỳ, B.; Tomášek, P.; Kiekintveld, C.; Kamhoua, C. Optimizing honeypot strategies against dynamic lateral movement using partially observable stochastic games. *Comput. Secur.* **2019**, *87*, 101579. [CrossRef]
69. Moothedath, S.; Sahabandu, D.; Allen, J.; Clark, A.; Bushnell, L.; Lee, W.; Poovendran, R. A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multistage Advanced Persistent Threats. *IEEE Trans. Autom. Control* **2020**, *65*, 5248–5263. [CrossRef]
70. Yang, L.X.; Li, P.; Yang, X.; Tang, Y.Y. A Risk Management Approach to Defending Against the Advanced Persistent Threat. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 1163–1172. [CrossRef]

71. Li, B.; Xiao, Y.; Shi, Y.; Kong, Q.; Wu, Y.; Bao, H. Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems. *IEEE Open J. Comput. Soc.* **2020**, *1*, 250–261. [CrossRef]
72. Zhang, M.; Zheng, Z.; Shroff, N.B. Defending against stealthy attacks on multiple nodes with limited resources: A game-theoretic analysis. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 1665–1677. [CrossRef]
73. Zhang, R.; Zhu, Q. FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2026–2041. [CrossRef]
74. Bakker, C.; Bhattacharya, A.; Chatterjee, S.; Vrabie, D.L. Hypergames and cyber-physical security for control systems. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 1–41. [CrossRef]
75. Tan, J.l.; Zhang, H.w.; Zhang, H.q.; Lei, C.; Jin, H.; Li, B.w.; Hu, H. Optimal Timing Selection Approach to Moving Target Defense: A FlipIt Attack-Defense Game Model. *Secur. Commun. Netw.* **2020**, *2020*, 3151495. [CrossRef]
76. Tian, W.; Ji, X.; Liu, W.; Liu, G.; Zhai, J.; Dai, Y.; Huang, S. Prospect theoretic study of honeypot defense against advanced persistent threats in power grid. *IEEE Access* **2020**, *8*, 64075–64085. [CrossRef]
77. Ye, D.; Zhu, T.; Shen, S.; Zhou, W. A differentially private game theoretic approach for deceiving cyber adversaries. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 569–584. [CrossRef]
78. Xie, Y.; Ji, L.; Li, L.; Guo, Z.; Baker, T. An adaptive defense mechanism to prevent advanced persistent threats. *Connect. Sci.* **2021**, *33*, 359–379. [CrossRef]
79. Yang, L.X.; Huang, K.; Yang, X.; Zhang, Y.; Xiang, Y.; Tang, Y.Y. Defense against advanced persistent threat through data backup and recovery. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2001–2013. [CrossRef]
80. Gao, Q.; Wu, H.; Zhang, Y.; Tao, X. Differential game-based analysis of multi-attacker multi-defender interaction. *Sci. China Inf. Sci.* **2021**, *64*, 1–13. [CrossRef]
81. Huang, L.; Zhu, Q. Duplicity games for deception design with an application to insider threat mitigation. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4843–4856. [CrossRef]
82. Feng, S.; Xiong, Z.; Niyato, D.; Wang, P. Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach. *IEEE Trans. Cloud Comput.* **2021**, *9*, 995–1007. [CrossRef]
83. Merlevede, J.; Johnson, B.; Grossklags, J.; Holvoet, T. Exponential discounting in security games of timing. *J. Cybersecur.* **2021**, *7*, tyaa008. [CrossRef]
84. Nisioti, A.; Loukas, G.; Rass, S.; Panaousis, E. Game-theoretic decision support for cyber forensic investigations. *Sensors* **2021**, *21*, 5300. [CrossRef]
85. Joshi, C.; Aliaga, J.R.; Insua, D.R. Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE TIFS* **2020**, *16*, 1131–1142. [CrossRef]
86. Bakker, C.; Bhattacharya, A.; Chatterjee, S.; Vrabie, D.L. Metagames and hypergames for deception-robust control. *ACM Trans. Cyber-Phys. Syst.* **2021**, *5*, 1–25. [CrossRef]
87. Mi, Y.; Zhang, H.; Hu, H.; Tan, J.; Wang, J. Optimal Network Defense Strategy Selection Method: A Stochastic Differential Game Model. *Secur. Commun. Netw.* **2021**, *2021*, 1–16. [CrossRef]
88. Tan, J.; Zhang, H.; Zhang, H.; Hu, H.; Lei, C.; Qin, Z. Optimal temporospatial strategy selection approach to moving target defense: A FlipIt differential game model. *Comput. Secur.* **2021**, *108*, 102342. [CrossRef]
89. Liu, X.; Zhang, J.; Zhu, P.; Tan, Q.; Yin, W. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Comput. Secur.* **2021**, *102*, 102138. [CrossRef]
90. Seo, S.; Kim, D. SOD2G: A Study on a Social-Engineering Organizational Defensive Deception Game Framework through Optimization of Spatiotemporal MTD and Decoy Conflict. *Electronics* **2021**, *10*, 3012. [CrossRef]
91. Xiao, L.; Xu, D.; Xie, C.; Mandayam, N.B.; Poor, H.V. Cloud storage defense against advanced persistent threats: A prospect theoretic study. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 534–544. [CrossRef]
92. Rass, S.; König, S.; Schauer, S. Defending against advanced persistent threats using game-theory. *PLoS ONE* **2017**, *12*, e0168675. [CrossRef]
93. Abass, A.A.A.; Xiao, L.; Mandayam, N.B.; Gajic, Z. Evolutionary game theoretic analysis of advanced persistent threats against cloud storage. *IEEE Access* **2017**, *5*, 8482–8491. [CrossRef]
94. Wan, Z.; Cho, J.H.; Zhu, M.; Anwar, A.H.; Kamhoua, C.A.; Singh, M.P. Foureye: Defensive Deception Against Advanced Persistent Threats via Hypergame Theory. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 112–129. [CrossRef]
95. Li, H.; Wu, J.; Xu, H.; Li, G.; Guizani, M. Explainable Intelligence-Driven Defense Mechanism Against Advanced Persistent Threats: A Joint Edge Game and AI Approach. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 757–775. [CrossRef]
96. Pawlick, J.; Zhu, Q. *Game Theory for Cyber Deception*; Springer: Berlin/Heidelberg, Germany, 2021.
97. Xiao, Q. Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study. *Telemat. Inform.* **2021**, *58*, 101535. [CrossRef]

98. Al-Kadhimi, A.A.; Singh, M.M.; Jabar, T. Fingerprint for Mobile-Sensor APT Detection Framework (FORMAP) Based on Tactics Techniques and Procedures (TTP) and MITRE. In Proceedings of the Eighth International Conference on Computational Science and Technology, Labuan, Malaysia, 28–29 August 2021; Springer: Singapore, 2022; pp. 515–533.
99. Jabar, T.; Singh, M.M.; Al-Kadhimi, A.A. Mobile Advanced Persistent Threat Detection Using Device Behavior (SHOVEL) Framework. In Proceedings of the eighth International Conference on Computational Science and Technology, Labuan, Malaysia, 28–29 August 2021; Springer: Singapore, 2022; pp. 495–513.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.