RESEARCH PAPER DOI: 10.22080/frai.2026.30929.1044

Journal of Future Research in Artificial Intelligence and Internet of Things

Journal Home page: https://frai.journals.umz.ac.ir/

Improving Cyber Security Situational Awareness Using Game Theory

Motahareh Dehghan [1*], Amir Mohammadhasani [2]

[1] *Department of Information Technology Engineering, Faculty of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran, ORCID: 0000-0002-5316-8005.*

[2] *Department of Information Technology Engineering, Faculty of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran.*

**Corresponding Author: m_dehghan@modares.ac.ir*

Article Info

Received 27 Dec 2025

Accepted 26 April 2026

Available online 12 Sep 2026

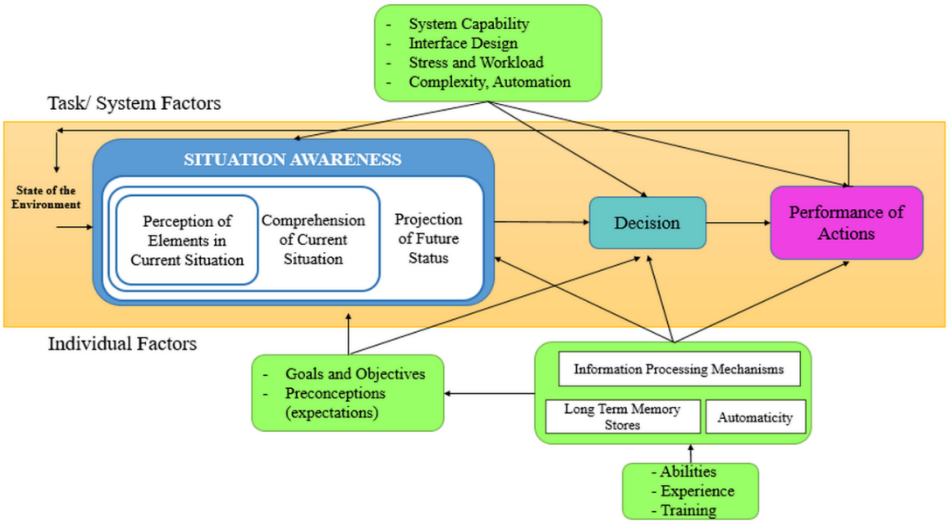
Keywords:

Situation Awareness;
Game Theory;
Endsley Model;
Stackelberg Game;
Cybersecurity;
Nash Equilibrium.

Abstract:

In today's digital era, situation awareness plays a vital role in strategic decision-making within dynamic and competitive environments and is recognized as one of the fundamental pillars of cybersecurity management. This study aims to analyze how situation awareness can be enhanced through the application of game theory concepts. It investigates the interactions between defenders and attackers, demonstrating how this mathematical framework can model the strategic dynamics between adversaries and defenders. Considering that situation awareness encompasses three levels—perception, comprehension, and projection—this research adopts Endsley's standard model as the primary framework. By integrating the concepts of game theory and Nash equilibrium, it reviews prior studies and explores the interrelationship between these two domains. The findings indicate that combining situation awareness with game theory can improve rapid responses to cyber threats and enhance decision-making under uncertainty. Moreover, this approach contributes to the efficient management of limited defensive resources, prediction of attacker behaviors, optimization of defensive reactions, and increased accuracy in attack detection. Finally, the study provides recommendations for developing integrated models, employing reinforcement learning algorithms, improving multi-source data management, and applying game theory to emerging areas such as the Internet of Things.

Graphical Abstract



ISSN 3092-7552

Please cite this paper as:M. Dehghan and A. Mohammadhasani, "Improving Cyber Security Situational Awareness Using Game Theory", Future Research in AI and IOT, vol. 2, no. 2, pp. 53-66.

1. Introduction

In today's world, with the advancement of information and communication technologies, digital systems have become an inseparable part of everyday life. These systems—from social networks to critical infrastructures such as power grids, water systems, and financial networks—play an essential role in the functioning of modern societies. In the current complex and dynamic environment, making strategic decisions under uncertainty is one of the greatest challenges. This issue becomes even more critical in cyber environments, where interactions between actors (such as attackers and defenders) are constantly evolving. Situation Awareness (SA), as one of the fundamental principles of cybersecurity management, plays a vital role in risk reduction and enhancing decision-making. Situation awareness refers to the accurate and timely understanding of an environment, existing conditions, hidden threats, and the prediction of future behaviors. Given the inherently dynamic and uncertain nature of cyber environments, analytical tools such as game theory can be employed to model interactions between actors and improve

situation awareness. Game theory, as a powerful mathematical framework, enables the analysis of various strategies and helps us make optimal decisions in competitive and complex environments. Integrating situation awareness with game theory can provide a comprehensive framework for understanding and analyzing dynamic and complex environments. This approach not only enhances real-time decision-making but also enables the design of intelligent and resilient systems against emerging threats.

The aim of this paper is to investigate the application of game theory in improving situation awareness. The key research questions include:

- How does situation awareness influence decision-making?
- How can game theory contribute to identifying and analyzing different situations?
- Which game-theoretic models and methods can enhance situation awareness?
- How can analytical tools such as game theory be used to model attacker–defender interactions?
- What strategies can be designed to improve situation awareness under uncertainty?

In this paper, we first examine the concept of situation awareness, followed by a discussion of cybersecurity situation awareness, its importance in organizations, and related methodological approaches. Then, fundamental concepts of game theory are reviewed. Subsequently, by studying previous research, the relationship between these two concepts is explored with the goal of enhancing cybersecurity in organizations. Furthermore, situation awareness literature from 2000 to 2025 has been studied, with a particular focus on works published between 2010 and 2025. The research sources include Scopus, ScienceDirect, and IEEE databases. Additionally, Persian books and articles related to this topic have been used. In the field of game theory, studies from 2012 to 2025 have been reviewed, with greater emphasis on works published after 2020.

2. Fundamental Concepts

2.1. Situation Awareness

Numerous models have been proposed for situation awareness; however, the most widely cited model was introduced by Mica Endsley in 1995. Situation awareness is defined as *"the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their future status."* [1]. Figure 1 provides a foundation for discussing situation awareness and its role in the overall decision-making process. According to this model, the individual's perception of relevant environmental elements—obtained either from system displays or directly through human senses—forms the basis of situation awareness.

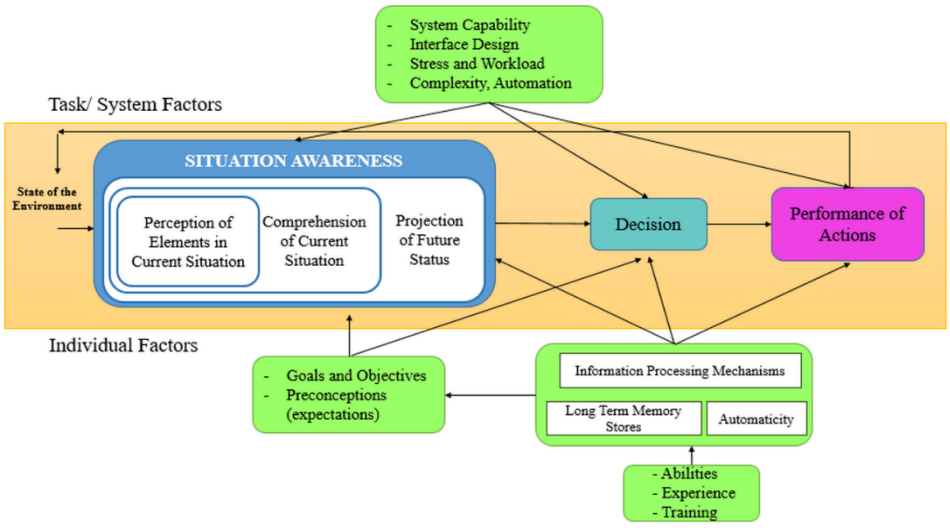


Figure 1. Situational Awareness Model in Dynamic Decision-Making [1]

The choice of action and performance are shown as distinct stages directly derived from situation awareness, although several other factors influence decision-making as well. Individuals differ in their ability to acquire situation awareness, even when presented with the same data inputs. This difference is assumed to stem from personal information-processing mechanisms influenced by inherent abilities, experience, and training. In addition, individuals may possess specific assumptions and goals that act as filters for interpreting the environment, shaping their situation awareness [1]. Cyber situation awareness consists of three key components:

Perception: identifying the occurrence of an attack along with its type, source, and target. This also includes awareness of data quality, accuracy, completeness, and timeliness.

Comprehension: assessing the current and future impacts of an attack (damage assessment). This component also involves understanding attacker behavior, including attack patterns and intent. Proper comprehension requires determining the underlying cause of the current situation.

Projection: anticipating how the situation will evolve and its potential consequences. A comprehensive situation awareness system helps decision-makers understand both the current state and the security posture of the system and improves their awareness up to the moment of action. Planning and executing response actions (after decision-making) rely on this understanding [2]. Despite its importance, most existing research approaches to achieving cyber situation awareness focus on lower and more abstract levels, such as vulnerability analysis using attack graphs, alert correlation, and intrusion detection techniques. Other approaches include analyzing attack trends, information flow, indicators, causality, forensics, and damage assessment [3]. However, higher-level situation awareness—ranging from comprehension to projection—remains largely undeveloped and is still performed manually by experts, which is time-consuming and error-prone. The lack of a dynamic, adaptive situation awareness system that can respond to changes in the environment without continuous human interaction remains a significant challenge [2].

2.2. Game Theory

Game theory, as a powerful mathematical framework, has become a critical tool for modeling strategic decision-making in competitive or cooperative settings. This theory, rooted in the foundational work of John von Neumann and John Nash, provides quantitative approaches for analyzing complex interactions between players, optimizing strategies, and predicting outcomes across diverse domains—from economics to computer science. In recent years, game theory has attracted significant attention in military defense due to its ability to translate high-level policies into operational strategies, evaluate multiple scenarios under predefined criteria, and align with emerging AI technologies. It not only supports decision-making under time pressure and high-risk conditions but also facilitates modeling in tracking systems, cyber warfare, air-ground combat, and resource management, paving the way for intelligent and secure decision-making systems in military environments [4]. Game theory encompasses various types, which are categorized and illustrated in Figure 2. In cybersecurity, game theory offers a unique opportunity to analyze strategic interactions between attackers and defenders. By formulating this dynamic as a two-player game, each party seeks to maximize its own payoff; the defender's strategy is shaped by the attacker's behavior, and vice versa. Game theory not only enables the optimization of defensive strategies through mathematically grounded models but also allows the design of mechanisms resilient to selfish behaviors, optimal resource allocation based on incentives, and the implementation of distributed solutions in decentralized networks [5]. Game theory helps us understand situations where decision-makers interact with one another. Although the term "game" may evoke everyday competitive activities governed by rules, the scope of game theory extends far beyond such simple interpretations [6]. Game theory is a branch of applied mathematics that focuses on analyzing and modeling strategic decision-making among rational entities (players) in competitive or cooperative environments. It assumes that players—based on available information, preferences, and strategies—seek to maximize individual or collective benefits, and the final outcome of a game depends on the interaction between their strategies. In general, a game consists of a set of rules, strategies, and payoffs associated with players' decisions, showing how a player or group of players can achieve the best possible outcome through specific combinations of actions [4]. Figure 3 illustrates the proposed architecture for decision-making in a cybersecurity situation awareness system using game theory. We present this architecture for the first time and, through a review of previous studies, aim to clarify the role of game theory in the field of cybersecurity situation awareness. The architecture combines attacker–defender interactions with game-theoretic analysis to evaluate costs, benefits, and strategic equilibria. Outputs from the situational awareness layer, including network assets, mission systems, and dependency relationships, are used as inputs to the game model. The attacker and defender strategies are mapped onto the network graph to identify critical nodes and possible attack paths. The game outcome highlights successful attacks and defenses, enabling the defender to allocate security resources optimally. This framework supports dynamic, risk-aware, and mission-oriented cybersecurity decision-making. The following section provides an overview of the related research conducted in this domain.

3. Related Work

Game-theoretic frameworks have been applied in various domains, including space situational awareness, cyber situational awareness, information situational awareness, surveillance, and detection. In each of these fields, situational awareness is supported by sensor-based estimations for state assessment, while the final state is shaped by the actions of multiple agents. Classical game theory assumes that players behave rationally within a well-defined environment; however, real-world conditions introduce variability stemming from social, cultural, and behavioral factors, making the system inherently uncertain [7]. Game theory provides a class of mathematical models that can be used in cyber situational awareness to study strategic interactions between attackers and defenders. In this research, we examine game-theoretic approaches within both design-oriented and application-oriented studies to present the current state of game theory in situational awareness systems and to

highlight its limitations. Fundamentally, the main goal of game-theoretic situational awareness is to predict the adversary's behavior against the defender.

Such prediction can offer a strategic advantage to the defender. Through game-theoretic analysis, a defender can theoretically identify the attacker's optimal strategy and consequently adopt the most effective defensive response [2]. Recent interdisciplinary research has increasingly integrated reinforcement learning (RL) with evolutionary game theory (EGT) to model adaptive, trial-and-error behavior in multi-agent systems [8]. In this paradigm—often termed RL-driven EGT—agents learn optimal strategies through environmental feedback rather than imitating neighbors' payoffs, thereby capturing more realistic learning dynamics observed in biological and social systems. While such models have successfully explained the emergence of cooperation in structured populations (e.g., via Q-learning or deep RL in spatial games), they fundamentally assume homogeneous agents, population-level interactions, and non-adversarial objectives. These assumptions render them ill-suited for cyber defense contexts, where adversaries are heterogeneous, strategically rational, and explicitly non-cooperative. In contrast, our work adopts a strategic (non-evolutionary) game framework—specifically, a Bayesian Stackelberg game—that explicitly models the defender's uncertainty over discrete attacker types (e.g., novice vs. APT) and optimizes commitment strategies under resource constraints. This distinction underscores a critical divergence: while RL-EGT explores how cooperation emerges, our model addresses how defense prevails in adversarial, information-asymmetric environments. [8].

3.1. Network Security Situational Awareness Models

Unlike traditional cybersecurity approaches, network security situational awareness provides a comprehensive method for identifying suspicious behavior within a network.

Through quantitative assessment of network security, this concept enables the inference of attacker intent, evaluation of attack impacts, and support for more effective decision-making. Network security situational awareness not only assists in detecting threats but also predicts the future trajectory of network security conditions. This capability is especially critical when confronting multi-stage and coordinated attacks, such as the Zeus botnet or targeted cyber worms. In recent years, network attacks have evolved from isolated patterns to sophisticated, multi-phase operations. These developments have made the study and advancement of network security situational awareness increasingly essential for detecting and responding to emerging threats. By providing a high-level perspective, network security situational awareness helps cybersecurity managers design more effective defensive strategies [9]. Although no universally accepted definition exists, network security situational awareness is generally understood as a process that identifies, analyzes, and evaluates key elements influencing network security, and forecasts future developments. Through quantitative security analysis, it offers a powerful decision-support tool for network administrators and enhances emergency response capabilities against cyber threats. Key advantages of network security situational awareness include:

Comprehensiveness: Providing a holistic view of network security status and all related events.

Accurate Attack Identification: Enabling effective and efficient detection of network-based attacks.

Real-Time Assessment: Allowing instantaneous detection and analysis of ongoing attacks, which is a core characteristic of network security situational awareness.

These capabilities make network security situational awareness a critical solution for protecting modern networks. It can transform the traditional pattern of active attacker–passive defender into a proactive and intelligent defensive paradigm [9].

Researchers have proposed a multi-sensor intrusion detection framework comprising intrusion detection, behavior analysis, intruder identification, scenario assessment, and threat evaluation. This framework is recognized as one of the earliest models of network security situational awareness. Inspired by Endsley's definition, the concept of network security situational awareness was further extended with a specific emphasis on network security considerations.

- **Network Flow–Based Situational Awareness Model**

Some researchers proposed a model based on network flow technology, enabling rapid identification of network weaknesses and threats. By providing a graphical representation of network conditions, the model enhances managerial oversight and situational visibility. However, challenges such as processing massive volumes of data remain significant issues requiring further investigation.

- **Situational Awareness Model for Large-Scale Networks**

For large-scale networks, researchers developed a situational awareness model that incorporates characteristics of big data. By integrating multi-source data analytics and advanced visualization techniques, this model enables administrators to identify and assess threats more effectively.
To illustrate this concept, an example of a four-level network security situational awareness model proposed in prior research is described below:

- **Level 1- Data Integration:** At this level, heterogeneous multi-source data are collected, preprocessed, and transformed into a unified format. Redundant or irrelevant information is removed to ensure consistency and quality.
- **Level 2- Correlation Analysis:** Using predefined rules from the network security knowledge base, correlations among security alerts are analyzed. This analysis evaluates vulnerabilities, assets, and event relationships and helps reduce the rate of false alarms.

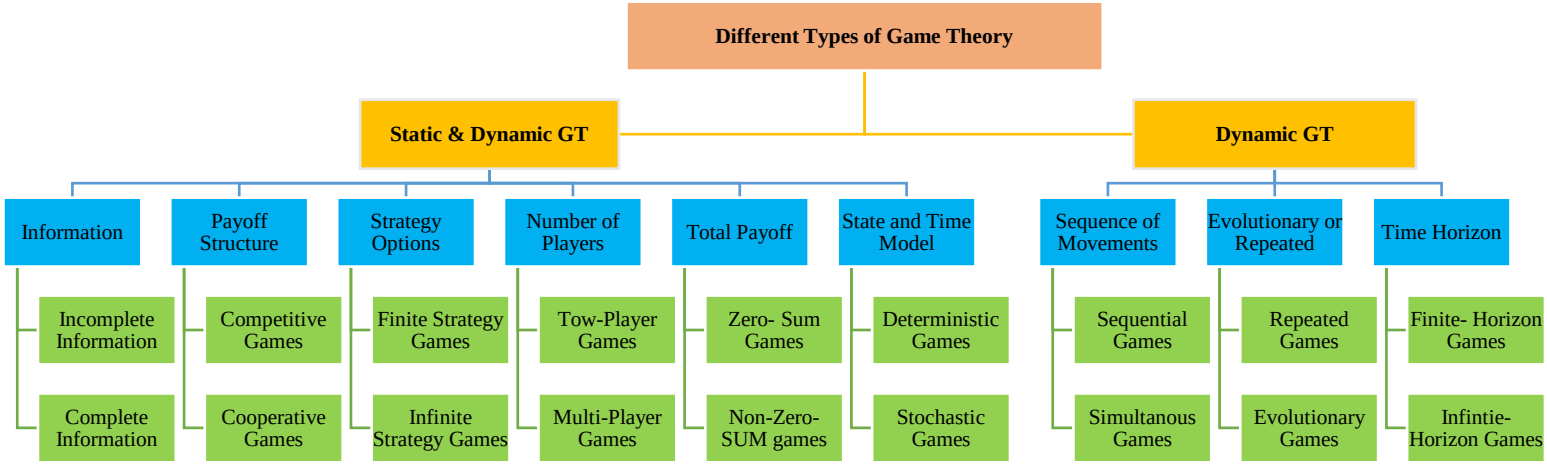


Figure 2. **Different types of game theory**

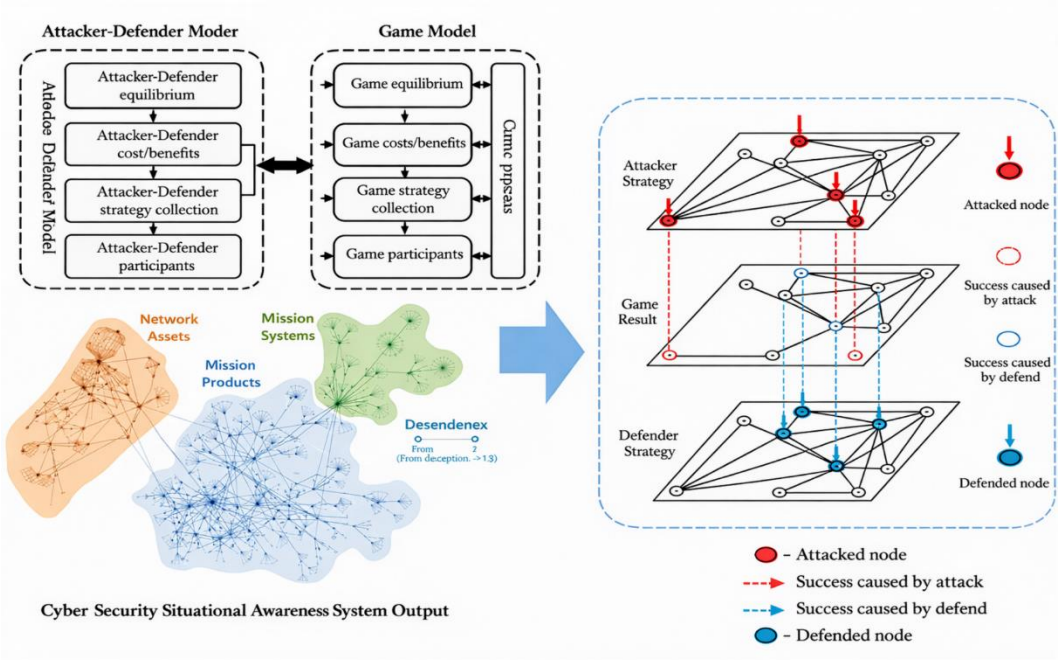


Figure 3. **Application of game theory in CSSA**

- **Level 3- Indicator System and Status Visualization:** In this level, security indicators (such as confidentiality, integrity, and availability) are computed using scientific methods, and the overall network condition is visualized. The network security index at time *t* is defined as Equation 1:

$$[C(t)I(t)A(t)] = [C_1C_2 \dots C_n; I_1I_2 \dots I_n; A_1A_2 \dots A_n] \quad [E_1(t); E_2(t); \dots; E_n(t)] \tag{1}$$

In this formulation, $E_i(t)$ represents the threat index of security event i at time t, while C(t), I(t), and A(t) denote the confidentiality, integrity, and availability indices, respectively.

- **Level 4- Situation Prediction:** Using historical data together with forecasting algorithms based on averages and trend analysis, this level predicts potential future security events.

3.2. Key Technologies in Network Security Situational Awareness

Key technologies in network security situational awareness are typically categorized into three functional components: status element collection, status assessment, and status prediction**.** This section examines these components and their associated technologies, highlighting strengths, limitations, and existing challenges.

- **Collection of Network Security Status Elements**

The collection of status elements forms the foundation of network security situational awareness. It involves gathering static data—such as network structure and vulnerabilities—as well as dynamic data, including threats and security event logs. Effective integration of these data sources enables holistic understanding and precise assessment of the network's condition. Research in this area can be grouped into two categories:

Single-Source Extraction: This approach focuses on specific types of data, such as vulnerability information or network alerts. For example, prior studies have used attack data or alert logs individually to assess security conditions. Due to its reliance on a single data source, this method lacks the ability to provide a comprehensive view of the network [10].

Multi-Source Extraction: More advanced approaches collect data from diverse sources with varying structures and hierarchies. Some researchers have proposed methods based on heterogeneous networks and non-negative matrix analysis for multi-source data integration [11]. Others have employed probabilistic neural networks to improve accuracy and efficiency in complex environments. Multi-source extraction techniques provide a more holistic understanding of network conditions and support more accurate threat analysis. However, single-source extraction remains incomplete due to limited data coverage. Multi-source methods, despite their strengths, face challenges such as inconsistent formats, standards, and data semantics, which necessitate extensive preprocessing, integration, and transformation. Additionally, irregular or large-volume data may reduce extraction efficiency. Other issues include low accuracy in identifying redundant data or false alarms, the limitations of offline methods for rapid response, and the need for targeted techniques such as demand-driven collection [9].

- **Network Security Situation Assessment**

Situation assessment forms the core of network security situational awareness. It analyzes multi-source security data and computes the network's security state based on mathematical models and formal logic. Similar to economic indicators, the resulting metric reflects the security posture of the network in a quantitative manner. Assessment methods fall into three main categories:

Mathematical Models: These methods rely on mathematical algorithms to evaluate the security state. The Analytic Hierarchy Process (AHP) is one of the most frequently used techniques. Researchers in [12] proposed a quantitative model for evaluating network threats comprising four layers: system, host, service, and attack. However, this model suffers from limitations due to its exclusive reliance on intrusion detection system (IDS) alerts and its omission of other data sources such as firewalls and system logs. Subsequent studies enhanced this model by integrating multi-source data to improve analytical accuracy. Other researchers introduced a multi-layer approach capable of reflecting security status over specific time intervals, although it is not suitable for real-time analysis [13].

Knowledge-Based Reasoning: Knowledge-based approaches rely on expert knowledge bases to analyze threats. These techniques draw upon fuzzy logic, Bayesian reasoning, and evidence theory. Some researchers proposed a fuzzy model combining AHP with fuzzy evaluation. Others used fuzzy inference models to assess security risks based on vulnerability, threat, likelihood, and impact factors, demonstrating the feasibility of the approach. Although these methods leverage artificial intelligence, they rely heavily on pre-defined inference rules and prior knowledge. Evidence theory, despite its simplicity in data fusion, becomes computationally complex when dealing with conflicting evidence. While these methods enable partial aggregation of network security status, they become inefficient when processing high-volume traffic or complex attacks characteristic of the big data era [14].

Pattern Recognition: Pattern-recognition-based approaches apply machine learning techniques to detect security-related patterns. This category includes methods such as grey correlation analysis, rough set theory, and clustering analysis. Some studies employed rough sets to reduce conditional attributes and derive decision rules, while hybrid rough-fuzzy approaches achieved improved computational accuracy [15]. Deep learning has gained prominence due to its flexibility and strong representational capacity [16]. For example, one study proposed an adversarial model combining deep autoencoders with deep neural networks, achieving higher accuracy in attack detection and more comprehensive assessment of network status [17, 18]. Although machine learning methods offer high efficiency and reduced dependency on expert knowledge, they still face challenges in extracting patterns from complex data, which may reduce their effectiveness. Hybrid approaches such as neuro-fuzzy networks can better capture dynamic changes in network conditions [9].

- **Network Security Situation Prediction**

Situation prediction uses historical data and current conditions to forecast future network security trends, transforming network defense from a passive to a proactive posture. Due to the nonlinear and stochastic nature of cyberattacks, traditional forecasting models often encounter difficulties. Prediction methods are generally divided into discrete models (attack graphs, Bayesian networks, hidden Markov models, game theory) and continuous models (machine learning, time-series analysis, support vector machines, and grey theory).

Attack Graphs: Attack graphs formally represent attack scenarios. Researchers have applied them to model potential attack paths, while others constructed graphs using maritime supply-chain information to identify probable access points.

Bayesian Networks: These are used to model the propagation of attacks and estimate vulnerability exploitation probabilities.

Hidden Markov Models (HMMs): Improved HMM variants have been introduced for more accurate prediction of network states. For example, a study proposed weighted HMMs for predicting the security state of mobile networks by incorporating multi-scale uncertainty, enhancing both training speed and prediction accuracy.

Game Theory: Game-theoretic models identify optimal defensive strategies against sophisticated attacks and support improved decision-making for network security managers.

Machine Learning: Offers strong self-learning and adaptability but requires abundant training data, and designing effective neural structures is challenging.

Markov Models: Well suited for time-series prediction but become impractical when enumerating all possible states in large-scale networks.

Grey Theory: Effective for short-term prediction with limited data, though restricted in complex network environments.

Support Vector Machines (SVMs): Known for strong generalization ability and fast convergence, making them excellent predictive tools, although parameter optimization remains a challenge.

3.3. Application of Game Theory in Network Security Situation Awareness

The application of game theory in analyzing and evaluating network security has attracted significant scholarly attention in recent years. While network security assessment focuses on analyzing vulnerabilities and threats, cyber situation awareness aims to provide a real-time and dynamic understanding of system conditions. Therefore, integrating game-theoretic models into situation awareness frameworks can offer a powerful tool for analyzing the strategic interactions between attackers and defenders. One of the common approaches in this area involves the use of Markov games and stochastic games, which are employed to model the dynamic and probabilistic behavior of agents in cyber environments. Early studies applied Markov games to design situation-awareness systems that detect attack patterns and estimate system states based on network-collected data. These studies demonstrated that game-theoretic models can yield a more accurate understanding of network conditions and provide more effective defensive strategies [7].

In other studies, Markov stochastic game models were proposed to quantify the level of network situation awareness. These models were designed around the interactions between attackers and defenders under different network-service states and were used to evaluate the payoff of both parties as well as the overall security posture. However, such models often suffer from scalability challenges in large state spaces; as network complexity increases, solving for state combinations becomes computationally expensive. Consequently, subsequent research aimed to develop models capable of handling larger and more dynamic environments, although scalability remains an open challenge.

Researchers later expanded the application of game theory to social networks**,** cloud environments, and dynamic systems. For example, White et al. [19] proposed a game-theoretic model to analyze multiple attack scenarios in online social networks. Using a Markov decision process, their model identified system vulnerabilities and recommended appropriate defensive mechanisms. Similarly, Zhang et al. [20] developed a Markov-game-based approach to enhance situation awareness by continuously gathering and analyzing threat-related data, asset information, and vulnerabilities. Their model considered users, network administrators, and attackers as three key actors and demonstrated high accuracy and efficiency in evaluating network conditions.

Other studies incorporated Nash equilibrium and fuzzy optimization to predict attacker behavior and strengthen defensive mechanisms in cloud environments. In another contribution, Ying et al. [21] introduced a dynamic situation-awareness system based on game theory, in which the attacker and defender were modeled as players in a stochastic game. By leveraging mathematical formulations of game theory, they quantified the costs and benefits of both parties and used the Nash equilibrium to determine an optimal balance between them.

Despite these promising outcomes, game-theoretic approaches still face several limitations. Assumptions of complete rationality among actors rarely hold in real-world environments, and available information is often incomplete or uncertain. These issues become more pronounced when dealing with advanced attackers who possess extensive environmental and behavioral knowledge. Therefore, scholars have suggested integrating game theory with machine learning and knowledge-driven approaches to enhance defensive and monitoring capabilities against sophisticated cyber threats [2].

Overall, game theory provides a systematic framework for analyzing strategic interactions between attackers and defenders. Within this framework, each party seeks to maximize its payoff by anticipating the actions of the opponent. Consequently, the effectiveness of any defensive mechanism depends on the reciprocal behavior and decisions of both sides. As noted by Du et al. [5], game theory serves as a powerful tool for modeling and analyzing strategic decision-making in network security and for examining the underlying motivations of cyberattacks.

3.4. Game-Theoretic Methodology for Cyber Defense Optimization

Kalderemidis et al. [22] introduce a game-theoretic methodology as a software-based tool for strengthening cyber defense and optimizing security budget allocation. This methodology integrates attack graphs, game theory, and the 0–1 knapsack problem to generate optimal defensive strategies. Attack graphs model multi-stage intrusion paths, while game theory—leveraging Nash equilibrium—simulates attacker–defender interactions. This tool enables Chief Information Security Officers (CISOs) to select appropriate security controls under budgetary constraints by treating each control as an independent decision variable. Evaluation of the methodology across multiple scenarios demonstrates its effectiveness against diverse cyber threats and attacker profiles.

The process begins with organizational asset risk analysis and proceeds to evaluate the effectiveness of security controls against known vulnerabilities. Using control games based on Nash equilibrium, the method optimizes budget allocation by formulating the problem as a multi-objective 0–1 knapsack model [23].

Previous studies largely focused on scenarios in which attackers pursue a single objective, offering limited insight into more realistic multi-objective attack scenarios. By integrating attack graphs with game theory, this methodology overcomes this limitation and enables optimal budget allocation for countering complex and multi-vector attacks. Through modeling multi-stage attack paths and simulating attacker–defender behavior, the method provides defensive strategies that have demonstrated practical effectiveness in real-world environments [24].

The proposed tool—referred to as the Game-Theoretic Model (GTM)—is designed to support a wide range of cybersecurity decision-makers, including CISOs, executives, IT analysts, board members, and security researchers. In this study, executives are assumed to be the primary users of the methodology, though detailed analysis of their roles and responsibilities is outside the scope of the research [25].

The game-theoretic methodology predicts all possible attack scenarios and utilizes game-theoretic reasoning to recommend optimal defensive strategies, enabling efficient allocation of limited cybersecurity budgets to reduce cyber risks. The tool consists of three main components:

Attack Graph Engine: This component generates attack graphs using vulnerability assessment reports (e.g., outputs from network vulnerability scanners such as Nessus). The graphs model all potential paths and states through which an attacker could compromise an organization.

Knowledge Base: This includes guidelines, rules, and reports related to cybersecurity and privacy, serving as a reference source for defense mechanisms. The knowledge base is periodically updated by CISOs, particularly after new incidents occur.

Defense Strategy Module: As the core of the methodology, this module simulates cyberattacks using game theory and attacker randomization profiles, computes the probability of each attack, and selects optimal security controls. It efficiently allocates limited budgets by optimizing control selection.

The game-theoretic defense strategy is based on zero-sum, state-independent games, enabling the methodology to model interactions between an organization (defender) and multiple potential attackers. The tool is resilient not only to technical vulnerabilities such as CVEs but also to common business-level weaknesses, making it versatile across diverse scenarios. By quantifying expected losses in monetary units, the tool helps decision-makers identify optimal security controls. Through modeling multiple threats for each asset and simulating attacker–defender interactions, it provides effective strategies for mitigating cyber risks [24].

The methodology was implemented as a prototype on Ubuntu 18.04 using Python on an AMD Ryzen 5 1400 processor with 8GB RAM. Results from 6,000 experimental runs show that GTM outperforms random and uncontrolled approaches by significantly reducing cyber risks through optimal budget allocation based on game theory and the 0–1 knapsack formulation [25].

3.5. Game Theory for Cyber Defense in Small and Medium-Sized Enterprises

In 2024, Kostelik examined cybersecurity challenges in small and medium-sized enterprises (SMEs) and proposed a game-theoretic framework that enhances managerial awareness of cyber threats and supports more effective strategic decision-making. In the digital era, SMEs face widespread threats due to limited resources and lack of expertise. The proposed framework increases managerial awareness of cyber risks such as social engineering, software vulnerabilities, and distributed denial-of-service attacks. Human factors, especially the role of managers in identifying, preventing, and responding to threats, are highlighted as central elements. Furthermore, the study considers both the technical and human dimensions of cybersecurity. Using a Bayesian game approach, the framework simulates interactions between attackers and defenders, enabling security managers to design more effective defenses against evolving and sophisticated threats [25]. An effective protective posture requires a multi-layered defense, combining technical and organizational measures. Some tasks can be executed by non-specialist managers, while others require specialized training. Crucially, managers must be capable of identifying the type of attack to select and implement the appropriate strategy [25]. The model incorporates sequential decision-making over time and simulates how strategies evolve as threats change. The reward matrices represent real-world outcomes such as financial losses, reputational damage, and regulatory penalties, making abstract decisions more tangible and actionable. This link between theory and practical consequences helps managers select realistic and effective strategies [25].

3.5.1. Illustrative Example: SME Manager Responding to a Cyber Threat

To demonstrate the practical application of game theory in SME cybersecurity management, the study presents a hypothetical scenario. A small cloud service provider with minimal security infrastructure and no dedicated security team experiences a phishing attack. The manager, who is solely responsible for security decisions, receives intrusion detection system alerts and

uses Bayesian updating—drawing on knowledge from a recent training course—to classify the attack. After analyzing suspicious email features, such as unusual links and attachments, the manager concludes that phishing is the most likely threat. Consequently, they choose a defensive strategy consisting of enhanced email filtering and an employee training session.

Over the following days, a decrease in suspicious activity confirms the effectiveness of the chosen strategy, leading the manager to update future strategy probabilities accordingly. The study further uses simulation data—generated from real security reports—to model strategic interactions between managers and attackers, creating a controlled environment for analyzing strategy choices and awareness evolution. This demonstrates how SME managers can strengthen cyber defenses using strategic models and dynamic learning, even without deep technical expertise [25].

The proposed framework is flexible and can be extended to more complex scenarios. Beyond independent attacks, it can model dynamic dependencies in which one attack becomes the starting point for subsequent attacks, enabling the simulation of more realistic attack patterns. The framework can also be expanded to cover other attack types, such as ransomware, by incorporating the likelihood, impact, and managerial response mechanisms into the game structure. This adaptability makes the model valuable for SMEs facing an ever-evolving cyber threat landscape [25].

Future research may integrate behavioral science, IT management, and data science to deepen understanding of strategic decision-making in dynamic cyber environments. Such an interdisciplinary approach not only enriches the theoretical framework but also supports the development of more robust, real-world cybersecurity strategies. Game theory serves as a practical tool for analyzing attacker–defender interactions in uncertain and rapidly changing environments, highlighting the importance of dynamic learning and situational awareness. The framework may be further enhanced by incorporating emerging threats such as AI-driven attacks or multi-attacker settings, as well as exploring adaptive learning mechanisms and scalability across organizational sizes. This study contributes to existing literature and lays the groundwork for future advances in strategic cyber defense [25].

The game-theoretic methodology is currently implemented as a prototype in Linux environments and has been evaluated through three case studies. Future plans include extending tool compatibility to Windows systems to reduce platform-related barriers. Planned algorithmic enhancements include integrating Best-First Search to identify attacker-optimal paths—thus improving defense prioritization—and incorporating Ant Colony Optimization to better identify critical system vulnerabilities. Future evaluations will focus on large-scale attack graphs representing extensive organizations with multiple attackers and targets in a zero-sum setting, examining return on investment for each node and its dependencies. These developments aim to strengthen the methodology's applicability in real-world and dynamic environments and support the creation of more advanced tools for cybersecurity and risk management [24].

3.6. Optimal Network Resource Allocation Using a Game-Theoretic Approach

Game theory is widely used to model strategic interactions between attackers and defenders in cyberspace. Its applications span numerous domains, including resource allocation, network security, and cooperative modeling. The resource allocation problem—commonly referred to as the allocation game—is a canonical game in cyber operations. In this context, the defender and attacker decide how to allocate their respective resources. Defender resources may include security infrastructure such as firewalls, antivirus systems, and other security controls. One of the defender's primary objectives is to allocate resources optimally to minimize both the likelihood of attack and unnecessary expenditure. Similarly, attackers may have limited resources or incur risks of detection and punishment for each offensive action.

Decision-making for optimal resource allocation in cyber warfare is highly complex, making game-theoretic models particularly useful for analyzing potential strategies. Given uncertain and incomplete information regarding states, costs, payoffs, and the impact of offensive and defensive actions, non-deterministic game-theoretic models are required to formulate cyber warfare scenarios. Expert belief degrees can be used to describe uncertain data when sufficient historical data or precise information about costs and payoffs is unavailable [24].

In real-world environments, decisions are usually made under uncertainty. Uncertainty refers to events whose outcomes are unknown until they occur. For instance, the outcome of a dice roll is inherently uncertain. The present work refers to key definitions and theorems in uncertainty theory that are useful for subsequent sections [24].

For modeling resource allocation in cyber warfare, game theory and uncertainty theory are combined to analyze attacker–defender interactions. The primary approach is to formulate the problem as a two-player Stackelberg game. Instead of relying on classical probability models, a quadratic integer programming framework with risk management criteria for worst-case scenarios is used. Decision confidence is incorporated into the model, which is enhanced by evaluating different defensive strategies. Ultimately, the model identifies an optimal Nash equilibrium between attacker and defender. This approach is suitable for national and international strategic decision-making and performs well under uncertain conditions. It is particularly applicable to scenarios with limited or imprecise data, allowing generalization to large-scale infrastructure and more informed decisions under incomplete information [24].

Game theory provides a logical framework for allocating security resources to prevent adversarial attacks and enables mathematical analysis of competitive situations. Stackelberg games are commonly used in limited-resource security allocation. In this model, the defender selects their strategy first, and the attacker subsequently chooses theirs with knowledge of the defender's decision. When the defender faces multiple attackers with different objectives, the game is formulated as a multi-objective optimization problem under uncertainty. Each objective function is optimized simultaneously, reflecting the real-world multi-goal nature of cybersecurity defense [25].

Experts' opinions are used to calculate the payoff for each player, considering factors such as target value, attack detection probability, and potential loss, all of which are uncertain. Uncertainty theory allows non-deterministic modeling, which is

more effective than classical statistics in security-related decisions. Using the weighted sum method—a common technique in multi-objective optimization—each objective is assigned a weight, and all objectives are linearly combined to reduce the multi-objective problem to a single-objective problem. In this research, this method is applied to transform multi-objective Stackelberg games into a single-objective optimization problem [25].

Through Stackelberg games, all potential strategies for both defender and attacker are examined. The defender optimally allocates resources based on probable attacker strategies to minimize overall risk. These methods have been applied in border security contexts [25].

3.7. A Game-Theoretic Model for Strategic Decision-Making in Cyber Warfare

Another study investigates the application of game theory in cybersecurity management using a two-player static game**.** The model derives optimal defensive strategies against cyberattacks while considering limited defensive resources. In this model, the attacker and defender simultaneously choose whether to attack or defend without knowledge of each other's decision. Each player's cost function is defined based on success probability, operational costs, and potential benefits. Optimal strategies are determined using Nash equilibrium analysis [26].

Results indicate that as the probability of defense success increases, the defender is more likely to invest in defense; conversely, high defense costs reduce the inclination to defend. Similarly, higher attack costs reduce the attacker's propensity to launch an attack. Sensitivity analysis shows that changes in game parameters, such as costs and success probabilities, directly influence optimal strategies. The algorithms developed can be applied in automated defensive systems and critical network environments [26].

The model assumes limited defensive resources, incomplete information about the opponent, and that each strategy has defined costs and benefits. The Nash equilibrium in this game is a mixed-strategy equilibrium, where both players act probabilistically depending on factors including defense cost, attack cost, and probabilities of successful defense or attack. This model has been applied in automated systems such as firewalls, enhancing defensive resource efficiency while ensuring system security [26].

3.8. Security Risk Assessment in Cyber-Physical Systems Using Game Theory

In the study by Sepehrzadeh [27], a decision-making framework is proposed for security risk assessment in cyber-physical systems (CPS)**,** specifically designed for situations where complete information about attackers or system security states is unavailable. In real-world environments, defenders often lack knowledge about the attacker's capabilities, motivations, or resources. Consequently, traditional risk models relying on complete or deterministic information are unrealistic.

To address this, the study employs a Bayesian game-theoretic approach, where attacker types (e.g., strong, medium, weak) are modeled as random variables, and the defender only possesses probabilistic beliefs about these types. First, the CPS structure, assets, vulnerabilities, and attack scenarios are modeled. A set of attack strategies and defense strategies is then defined, and for each combination, costs, payoffs, and attack outcomes are calculated. The Bayesian game captures the strategic interaction under uncertainty, and the Bayesian Nash equilibrium identifies the optimal defensive strategy that minimizes the defender's expected cost across all attacker types.

This process yields a quantitative risk assessment, simultaneously considering attack probability, potential impact, and defense effectiveness. Results show that this approach enables more realistic and informed security decisions, as defense strategies are aligned with optimal attacker behavior and defender beliefs, rather than simplifications or heuristic guesses. The framework is applicable across diverse domains including energy grids, industrial control systems, intelligent transportation, and industrial IoT, helping managers and analysts optimize defensive resource allocation and reliably quantify risk under uncertainty. Table 1 reviews the previous studies.

Table 1. Review of Previous Studies

Author(s) & Year	Research Content and Key Findings
Junwei Zhang et al., 2023	This paper provides a comprehensive review of the current state and recent advances in network security situational awareness (SA). It analyzes models, key technologies, and existing challenges. Network security SA is identified as a growing research area, highlighting the need to improve emerging technologies such as IoT, machine learning, and network security visualization systems.
Bentian Li et al., 2020	The study investigates the integration of heterogeneous networks to enhance situational awareness of network devices. Game-theoretic models are applied to analyze strategic interactions among nodes in such networks. Combining these approaches offers deeper insights into node behavior and decision-making in complex network environments.
Blasch et al., 2015	This article explores the applications of game theory in various domains of situational awareness, including spatial and cyber SA. It emphasizes that SA is supported by sensor estimations and multi-player assessments. Future developments in knowledge awareness, multi-scale analysis, and software methodologies are highlighted to enable new systems and games.
CUONG T. DO et al., 2017	The paper reviews game-theoretic approaches in cybersecurity and privacy, categorizing them into security and privacy domains, with a focus on CPS security and secure communications. It identifies emerging research trends and proposes combining existing knowledge with new developments as a novel approach to solving cybersecurity and privacy challenges. Game theory links to SA in analyzing actor behavior, developing optimal defensive strategies, threat prediction, and real-time decision-making.
Ioannis Kalderemidis et al., 2022	This study introduces a game-theoretic methodology as a tool for deriving optimal defensive strategies and security investment plans. Using attack graphs, game theory, and the 0-1 knapsack algorithm, it supports optimal budget allocation. The methodology allows information security managers to automatically generate effective defense strategies against diverse attackers, achieving maximum protection at minimal cost.
Sepehrzadeh, 2022	The paper presents a quantitative method for security risk assessment in cyber-physical systems (CPS) under incomplete information about attackers. Bayesian game theory is used to model attacker–defender interactions, where the defender only holds probabilistic beliefs about attacker types (e.g., capability, skill, intent). Attack scenarios, costs, impacts, and defense strategies are

	quantitatively defined, and Bayesian game equilibrium determines the optimal defensive strategy. The framework provides quantitative risk evaluation and optimization under uncertainty, demonstrating Bayesian game theory as a powerful tool for CPS risk management.
Kostelic, 2024	This study proposes a theoretical framework to analyze the role of situational awareness in strategic interactions between managers and attackers in cybersecurity. It emphasizes the impact of awareness on strategic choices and outcomes. Accurate threat assessment and understanding of attacker behavior are critical for effective decision-making. Results show that improved modeling of situational awareness enhances managerial decision-making and underscores the need for future research in emerging cyber threats.
Afrashteh & Zare Chavoshi, 2020	The paper investigates optimal resource allocation in cyber warfare using game theory. Two non-deterministic models are proposed for analyzing complex cybersecurity scenarios. The study suggests applying these approaches for developing optimization and simulation models of real-world cyber battles.
Partovi, 2019	This research studies multi-objective security games under uncertainty, employing game theory and Stackelberg models for optimal allocation of limited security resources. The weighted sum method is proposed to determine equilibrium points, and an application example is provided in border security.
Foroughi et al., 2018	The study examines decision-making processes in cyber conflicts using game theory and analytical modeling. It demonstrates that players can identify each other's vulnerabilities to choose optimal strategies. The model predicts adversary behavior and serves as a tool for designing appropriate strategies under varying conditions, though further research is needed to accurately estimate probabilistic variables.

4. Conclusion

The primary objective of this study was to gain a deeper understanding of how game theory concepts can be utilized to enhance situational awareness (SA) in dynamic and complex environments, as well as to provide a strategic decision-making tool. In Section 2, Endsley's SA model was employed as a standard framework. This model, with its three levels of perception, comprehension, and projection, effectively captures the SA process. The relationship between SA and decision-making was also examined, highlighting the influence of factors such as information volume, system interface design, stress, decision automation, and individual capabilities.

Game theory was introduced as a mathematical and strategic tool to model interactions among players, including attackers and defenders. Key concepts such as Nash equilibrium and zero-sum/non-zero-sum games were discussed, providing a foundation for analyzing various strategic scenarios. Section 3 reviewed previous studies, demonstrating practical applications of game theory in areas such as cybersecurity, resource allocation and management, training and skill enhancement for security managers, and cyber warfare systems. These studies showed that strategic game models can support adversary behavior prediction, optimal allocation of defensive resources, and rapid response to threats. Moreover, integrating artificial intelligence and machine learning with game theory enables the development of intelligent and self-learning systems. Despite these advancements, several limitations remain in the field:

Modeling complexity: Cyber-environment interactions are highly dynamic and uncertain, posing significant modeling challenges.

Need for real-world data: Many models require empirical data for validation, which may be difficult to obtain.

Computational constraints: Certain game-theoretic models are computationally intensive and may not scale effectively for large systems.

One of the most critical challenges identified is the uncertainty in input information and the complexity of operational environments. This underscores the need for efficient methods for data management, integration, and prediction of future behaviors. Based on the findings of this study, several directions for future research are proposed:

Evolutionary games for modeling dynamic behaviors: Given the high dynamism of cyber environments, evolutionary games can help model adaptive behaviors and the long-term learning of optimal strategies.

Optimizing defensive strategies through game theory and reinforcement learning: Combining reinforcement learning with game-theoretic approaches can develop intelligent defense systems capable of learning from past interactions and autonomously improving strategies.

Enhancing decision-making in cybersecurity SA systems via game theory: Integrating SA concepts with game theory can improve strategic decision-making in cybersecurity SA systems. This study demonstrates that combining situational awareness with game theory can enhance strategic decision-making in complex and dynamic environments, providing an effective model for strengthening cyber SA. The proposed approach allows modeling of complex interactions among multiple factors and assists in identifying and selecting optimal strategies under uncertainty.

Given the increasing complexity of digital systems and the growing sophistication of cyber threats, such a framework can serve as a practical tool across various security and management domains. The integration of these two fields supports the design of intelligent and adaptive defense systems capable of predicting adversary behavior and responding appropriately to emerging threats.

Ultimately, this research provides a theoretical foundation for further investigations into enhancing situational awareness using game-theoretic models. Although challenges remain in implementing such models, the outcomes offer significant potential for the development of practical and applicable solutions in the future.

5. Statements & Declarations

5.1. Author Contributions

Conceptualization, M.D. and A.M.; methodology, A.M.; validation, M.D. and A.M.; investigation, A.M.; resources, M.D.; data curation, A.M.; writing—original draft preparation, A.M.; writing—review and editing, M.D.; visualization, A.M.; supervision, M.D.; project administration, M.D. All authors have read and agreed to the published version of the manuscript.

5.2. Data Availability Statement

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

5.3. Funding

This research received no external funding.

5.4. Acknowledgments

The authors would like to express their sincere gratitude to the journal reviewers for their careful evaluation of the manuscript and their constructive comments and suggestions, which helped improve the clarity, quality, and overall presentation of the paper.

5.5. Declaration of Generative AI and AI-assisted Technologies in the Writing Process

The authors declare that during the preparation of this manuscript, AI-assisted technologies—specifically Qwen (developed by Alibaba Cloud)—were used solely for language refinement, grammatical correction, and improvement of academic phrasing in English. These tools were not involved in any aspect of scientific reasoning, conceptual development, theoretical modeling (including the Bayesian Stackelberg game formulation), data analysis, or decision-making regarding the research design. The authors take full responsibility for the originality, validity, and integrity of all content presented in this work.

5.6. Ethics Approval

Not applicable.

5.7. Informed Consent

Not applicable.

5.8. Consent for Publication

The authors consent to the publication of this manuscript.

5.9. Conflicts of Interest

The authors declare no conflict of interest.

6. References

[1] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” Situational Aware., vol. 37, no. 1, pp. 9–41, 2017, doi:10.4324/9781315087924-3.

[2] H. Alavizadeh et al., “A Survey on Cyber Situation-Awareness Systems: Framework, Techniques, and Insights,” ACM Comput. Surv., vol. 55, no. 5, p. 102828, 2023, doi:10.1145/3530809.

[3] M. Dehghan and E. Khosravian, “Advancing Situation Awareness Systems: Evaluating Decision-Making Methods with UAV Applications,” Manag. Strateg. Eng. Sci., vol. 6, no. 4, pp. 122–133, 2024, doi:10.61838/msesj.6.4.13.

[4] E. Ho, A. Rajagopalan, A. Skvortsov, S. Arulampalam, and M. Piraveenan, “Game Theory in Defence Applications: A Review,” Sensors, vol. 22, no. 3, p. 1032., 2022, doi:10.3390/s22031032.

[5] C. T. Do et al., “Game Theory for Cyber Security and Privacy,” ACM Computing Surveys, vol. 50, no. 2, pp. 1–37, May 2017, doi: 10.1145/3057268.

[6] M. J. Osborne, “An introduction to game theory, ” Oxford University Press, Oxford, United Kingdom, 2000.

[7] E. Blasch, D. Shen, K. D. Pham, and G. Chen, “Review of game theory applications for situation awareness,” Sensors and Systems for Space Applications VIII, vol. 9469, p. 94690I, May 2015, doi:10.1117/12.2177531.

[8] K. Xie and A. Szolnoki, “Reinforcement learning in evolutionary game theory: A brief review of recent developments,” Appl. Math. Comput., vol. 510, p. 129685, 2026, doi:10.1016/j.amc.2025.129685.

[9] J. Zhang, H. Feng, B. Liu, and D. Zhao, “Survey of Technology in Network Security Situation Awareness,” Sensors, vol. 23, no. 5, p. 721, 2023, doi:10.3390/s23052608.

[10] W. Hailong and G. Zhenghu, “Heterogeneous Multi-sensor Information Fusion Model for Botnet Detection,” 2010 International Conference on Intelligent Computation Technology and Automation, pp. 428–431, May 2010, doi:10.1109/icicta.2010.575.

[11] B. Li, D. Pi, Y. Lin, I. A. Khan, and L. Cui, “Multi-source information fusion based heterogeneous network embedding,” Information Sciences, vol. 534, pp. 53–71, Sep. 2020, doi:10.1016/j.ins.2020.05.012.

[12] Y. Jia, H. Wu, and D. Jiang, “A Hierarchical Framework of Security Situation Assessment for Information System,” 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 23–28, Sep. 2015, doi:10.1109/cyberc.2015.47.

[13] H. Zhang, C. Kang, and Y. Xiao, “Research on Network Security Situation Awareness Based on the LSTM-DT Model,” Sensors, vol. 21, no. 14, p. 4788, Jul. 2021, doi:10.3390/s21144788.

[14] D. Kong, H. li, and H. dong, “Research on Network Security Situation Assessment Technology Based on Fuzzy Evaluation Method,” Journal of Physics: Conference Series, vol. 1883, no. 1, p. 012108, Apr. 2021, doi:10.1088/1742-6596/1883/1/012108.

[15] C. Li and X. M. Li, “Cyber performance situation awareness on fuzzy correlation analysis,” 2017 3rd IEEE International Conference on Computer and Communications (ICCC), pp. 424–428, Dec. 2017, doi:10.1109/compcomm.2017.8322583.

[16] A. Safdel, J. Ghasemi, and S. A. Zendehbad, “Advanced Deep Learning Approaches for Accurate and Efficient Suspicious Behavior Detection in Surveillance Videos,” Comput. Sci. Eng., vol. 4, no. 2, pp. 203–216, 2025, doi:10.22124/cse.2025.30210.1099.

[17] H. Yang, R. Zeng, G. Xu, and L. Zhang, “A network security situation assessment method based on adversarial deep learning,” Applied Soft Computing, vol. 102, p. 107096, Apr. 2021, doi:10.1016/j.asoc.2021.107096.

[18] M. Dehghan, B. Sadeghian, E. Khosravian, A. S. Moghaddam, and F. Nooshi, “ProAPT: Projection of APTs with Deep Reinforcement Learning,” ISeCure, vol. 17, no. 1, pp. 25–41, 2025, doi:10.22042/isecure.2024.428569.1052.

[19] J. White, J. S. Park, C. A. Kamhoua, and K. A. Kwiat, “Game theoretic attack analysis in online social network (OSN) services,” Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 1012–1019, Aug. 2013, doi:10.1145/2492517.2500257.

[20] YZhang, Y., Tan, X. B., Cui, X. L., & Xi, H. S, “Network security situation awareness approach based on Markov game model,” Procedia Engineering, vol. 22, no. 3, pp. 495–508, 2011, doi: 10.3724/SP.J.1001.2011.03751.

[21] L. Ying, L. Bingyang, and W. Huiqiang, “Dynamic awareness of network security situation based on stochastic game theory,” The 2nd International Conference on Software Engineering and Data Mining (SEDM), pp. 101–105, June 2010.

[22] I. Kalderemidis, A. Farao, P. Bountakas, S. Panda, and C. Xenakis, “GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments,” Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1–9, Aug. 2022, doi:10.1145/3538969.3544431.

[23] K. Kostelić, “Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach,” Games, vol. 15, no. 2, p. 13, Apr. 2024, doi:10.3390/g15020013.

[24] E. Afrashteh and A. Zare Chavoshi, “Optimal resource allocation in cyber warfare with a game theory approach in uncertain environment,” Iranian Journal of Wargaming, vol. 3, no. 6, Art. no. e128131, 2020., doi:10.22034/ijwg.2020.128131.

[25] M. R. Mehregan, M. R. Khorashadizadeh, and M. T. Partovi, “Optimal allocation of security resources by using game theories,” Iranian Journal of Wargaming, vol. 2, no. 4, pp. 41–55, 2019. doi:10.22034/ijwg.2019.97247.

[26] S. Shiva, S. Roy, and D. Dasgupta, “Game theory for cyber security,” Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, pp. 1–4, Apr. 2010, doi:10.1145/1852666.1852704.

[27] H. Sepehrzadeh, “A method for assessing security risk in cyber-physical systems with incomplete information using Bayesian game theory,” Karafen Sci. J., vol. 19, no. 1, pp. 495–521, doi:10.48301/kssa.2022.320681.1909.