IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

# Correlating Decision Theory with Cyber Threat Intelligence: Novel Perspectives

**Neha Akella[1], Manas Kumar Yogi[2]**

[1]B.TECH III Year CSE-AI &ML Department, Pragati Engineering College (A), Surampalem, A.P., India

[2]Assistant Professor CSE Department, Pragati Engineering College (A), Surampalem, A.P., India

**E-mail:** [1]akellaneha@gmail.com, [2]manas.yogi@gmail.com

## Abstract

An organization, with the help of cyber threat intelligence framework, can protect itself from the cyber threats. The stakeholder cyber safety is paramount and such intelligence frameworks help leveraging the business value of its intellectual properties. Events related to securing the cyber aspects of an organization are possible by connecting it with essential features of decision theory. Few assumptions are made pertaining to descriptive, prescriptive and normative decision theory which help in identification of cyber weakness and security loopholes of an organization. This study extracts novel viewpoints from the strongholds of decision theoretical models and propagates decisions on how to face the cyber-attacks.

**Keywords:** Cyber Security, Cyber Threat Intelligence (CTI), Denial of Service, Decision Theory.

## 1. Introduction

In today's fast-paced world, the reliance on computer systems and technology has significantly increased. As a result, the risk of cyber threats is ever-present. A cyber threat encompasses malicious activities and tactics employed by individuals or groups to harm digital assets or data. These threats come in various forms such as malware, phishing attacks, ransomware, and Denial of Service (DoS) attacks. The consequences can be severe, potentially impacting the confidentiality, availability, and integrity of valuable digital assets. Furthermore,


*DOI: https://doi.org/10.36548/jsws.2023.3.004*
*Received: 05.09.2023, received in revised form: 24.09.2023, accepted: 10.10.2023, published: 25.10.2023*

modern cybercriminals utilize advanced tactics, techniques, and procedures (TTPs) that are challenging to detect, investigate and resolve. For example, the wannacry ransomware attack that started on May12,2017, spread over 150 countries within a day and infected more than 230,000 computers [1]. Why do cyber-attacks thrive? It is because cyber-attacks are less risky and cheaper compared to physical attacks. Due to the anonymous nature of the internet it is challenging to trace and identify the attackers.

### 1.1 Need for CTI

In response to the growing number of cyber threats worldwide and the shortcomings of traditional security approaches, organizations are incorporating cyber threat intelligence (CTI) efforts. CTI represents an *actionable threat information* designed for a particular organization needing careful attention and prevention [2]. The actionable threat intelligence offers enough information to make an informed decision that can be acted upon. CTI consists of activities to gather relevant threat information for a specific organization to engineer more precise defense strategies. The data includes the information about the threat types, sources, the technologies employed, and the methods of attack [2].

### 1.2 CTI Techniques

CTI techniques help organizations better understand potential threats, make informed decisions and enhance their overall cybersecurity protection. CTI provides in-depth information about cyber-attacks that may occur. For example, an email designed for phishing attacks could contain details such as the attack technique used, attacker information, target information, software, and tools used to launch the attack [3]. CTI has three levels: strategic, operational, and tactical.

- *Strategic CTI* provides a high-level overview of the cyber threat landscape and the organization's position within it. This enables decision-makers to better grasp the cyber risks they encounter and their possible outcomes.
- *Operational CTI* reveals the tactics, techniques, and procedures (TTPs) used by threat actors. It also uncovers their motives, targets, and attack behaviors. This facilitates the building of better defences.
- *Tactical CTI* identifies the specific indicators of compromise (IOCs) that signal an active breach. It helps security tools automatically block or mitigate attacks.

### 1.3 CTI Tools

Cyber threat intelligence tools are the technologies designed to support various aspects of cyber threat intelligence activities. The CTI tools can be categorized into two functional groupings namely the tools for processing data and turning it into intelligence, and tools for managing intelligence including generating alerts based upon intelligence [4].

#### Processing Tools

Processing tools are essential for converting raw information into actionable intelligence. These tools play a crucial role in data analysis and informed decision-making. These tools handle tasks like deduplication, data enrichment, and reverse engineering of malware [4].

#### Management Tools

Management tools provide the functionalities to support decision-making, incident response, and overall cyber security activities. These tools include SIEM platforms, network traffic monitoring tools, intrusion monitoring platforms, forensics platforms, and third-party visualization tools [4]. According to 2022 Sans Cyber Threat Intelligence (CTI) Survey, network traffic monitoring tools and intrusion monitoring platforms are extensively employed tools in the field. The Security Information and Event Management (SIEM) platform stands out with the highest level of usage at 86.9% and remarkable degree of automation.

### 1.4 Relevance of Decision Theory in Aiding Effective Decision-Making

In the complex realm of cyber threat intelligence (CTI), the integration of Decision Theory presents itself as a guiding light for enhancing the decision-making procedures. Decision Theory provides a structured methodology to comprehend how individuals and organizations navigate decision-making amidst uncertainty. These methodologies include Game Theory, Expected Utility Theory, Prospect Theory, Satisficing Theory and Heuristics. Decision Making involves selecting the optimal course of action from alternatives. The decision-making process involves the following steps – Problem Detection, diagnosis, decision criteria establishment, alternatives development and evaluation, implementation and assessment. With Decision Theory and these methods, organizations can decipher the tricky

puzzle of cyber threats and build strategies to strengthen their resilience against evolving hazards.

This paper aims to explore the correlation between decision theory and cyber threat intelligence and how this relationship can enhance cybersecurity. Initially, literature survey covering the fundamental knowledge of Decision Theory, its benefits, and how Decision Theory can be applied in the field of CTI is presented. Then the impact of Decision Theory in the design and development of CTI and understand the Cyber Threat Intelligence frameworks is illustrated. Finally, a closer look at the current limitations and gaps in integrating decision theory in CTI and further enhancements is presented.

## 2. Literature Survey

Cyber Threat Intelligence (CTI) is the knowledge and understanding of actual or perceived threats that inform organization's security decision making [5]. It is a relatively new discipline used in very few sectors such as banking, finance, government and technology. On the other hand, Decision Theory which stems from probability theory and analytic philosophy delves into the theoretical aspects of decision-making. It involves assigning probabilities to different factors and numerical consequences to the outcome. In the context of cyber security, integration of decision theory has proven to be extremely valuable in countering cyber threats, and its significance is continuing to grow. This study aims to address two critical questions:

Q1. How can Decision Theory be practically implemented in the field of CTI?

Q2. What are the current limitations and gaps existing in decision theory models when applied to cyber threat scenarios? To answer these, a comprehensive literature survey is conducted. the benefits of decision theory and its applications in countering cyber threats are briefly presented. The table .1 illustrates the Primary sources and Secondary sources gathered for the study about the decision theory.

**Table 1.** Primary Sources and Secondary Sources Gathered for the Study about the Decision Theory

| Reference No. | Source of Information | Application of Decision Theory | Application in Cyber Security |
|---|---|---|---|
| [5] | Primary-Research papers | Expected Utility Theory (EUT) | Intrusion detection |
| [6] | Primary-Case Studies | Regret Theory | Incident response |
| [7] | Primary-Experimental Studies | Rank-Dependent Utility Theory | Intrusion detection |
| [8] | Primary-Interviews and Surveys | Decision Trees | Threat intelligence |
| [5] | Secondary-Books | Game Theory | Threat intelligence, Threat Assessment |
| [6] | Secondary-Online Blogs | Bayesian Decision Theory | Security investments, Risk Management |
| [7] | Secondary-Review articles | Fuzzy Logic | Incident response, Intrusion detection |
| [7] | Secondary-Encyclopedias and Reference Works | Markov Decision Process (MDP) | Security investments, Risk Management |

## 2.1 Current Challenges in CTI

- **Threat Data Overload**

One of the biggest challenges is threat data overload. A vast amount of data is accessible from various sources, making it difficult for the organizations to effectively analyze and keep pace with it all. This can result in crucial threats being overlooked or wasting time on false positives.

- **Threat Data Quality**

CTI analysts collect data from various sources, not all threat data is reliable or actionable. Some threat data maybe outdated, inaccurate or incomplete. Consequently, organizations can face challenges in making informed decisions regarding their response strategies to these threats.

- **Privacy and Legal Issues**

Organizations need to be careful about sharing CTI data, as it may contain sensitive information. This can make it difficult to collaborate on threat intelligence and share information with other organizations.

## 2.2 Foundational Concepts of Decision Theory

Decision Theory looks at decision-making from three perspectives, namely normative, descriptive, and prescriptive. These perspectives provide a thorough grasp of how individuals and organizations make choices in the decision-making process [6].

- **Normative Perspective: Defining Rational Choices**

The normative perspective of Decision Theory is concerned with "how decisions should be made" considering rational choices. It sets forth the criteria and principles for making decisions when faced with uncertainty or ambiguity [6].

- **Descriptive Perspective: Understanding How People Make Decisions**

The descriptive perspective of Decision Theory reflects "how people actually make decisions". It seeks to uncover patterns, biases, and cognitive heuristics that influence decision-makers. The descriptive methods provide case-specific insight into areas that require improvement [6].

- **Prescriptive Perspective: Developing Decision-Making Aids**

The prescriptive perspective of Decision Theory is concerned with the practical application of decision models. It involves the investigation and development of models and decision aids for facilitating better choices. It draws from both normative and descriptive perspectives to create practical solutions and enhance decision quality [6].

## 2.3 Benefits of Decision Theory

Decision theory provides several important benefits that greatly influence cybersecurity activities. By applying Decision Theory models, organizations can efficiently identify and assess potential risks. Decision Theory provides with a valuable tool: the risk matrix. The risk matrix is a table that consists of the severity, likelihood and impact of each risk. It helps in visualizing and prioritizing the risk landscape. Through the application of decision models, organizations can strategically determine where to invest their budget, personnel and technology resources based on the severity and likelihood of different cyber threats.

Moreover, Decision Theory equips organizations with the agility needed to develop dynamic defense strategies, capable of thwarting and evolving cyber threat scenarios. Furthermore, Decision theory expedites quick and effective incident response, reducing the response time and thereby minimizing the impact of cyber-attacks. Decision theory opens the door to the investigation of cyber criminals' and victims' motives, preferences, and biases. This information can then be used to develop advanced strategies and tools in the ongoing battle against cyber threats.

### 2.4 Applications of Decision Theory in Countering Cyber Threats

One of the key challenges in cybersecurity is making decision under uncertainty. Uncertainty arises when a person lacks complete knowledge about future events or outcomes. In such situations, Decision Theory can be employed for making optimal decisions. In this section,some of the areas where decision theory can be applied to counter the cyber threats is explored:

#### 2.4.1 Risk Assessment

Cybersecurity decision makers use decision theory techniques such as Utility Theory to identify potential cyber threats and vulnerabilities in an organization that could be the entry points for the attackers. Utility theory enables them to assess the possible consequences of cyber threats and their impact based on the utilities they assign to different outcomes [7]. For example, in the banking sector, decision theory is used to evaluate the risk of a customer default loans. The bank analyses various factors such as the income, debt levels and credit history of the customer. Consequently, decisions are made regarding loan approval and determining appropriate interest rate.

### 2.4.2 Intrusion Detection

Intrusion detection methods are employed to monitor the system and network conditions, effectively identifying any suspicious or unauthorized activities that may threaten their security. Decision theory models such as Bayesian Networks, are utilized by companies to detect intrusions into their networks. Bayesian networks use probability theory to analyze the data effectively and infer the likelihood of intrusion based on the evidence and prior knowledge [8].

### 2.4.3 Cybersecurity Investment

The goal of cyber security investment is to safeguard an organization against cyber threats by allocating necessary resources. Developing holistic approaches is crucial to assess risks effectively and find the best cybersecurity solutions. Game theory as a subfield of Decision theory plays a crucial role in cyber security investment in two ways. Firstly, to analyze the trade-off between cozy and benefit of security measures. Secondly, it allows organizations to understand how information asymmetry impacts decision-making [9,10].

### 2.4.4 Threat Hunting

Cyber threat hunting (CTH) is a proactive and innovative methodology for detecting cyber threats. It combines the utilization of cyber threat intelligence (CTI) methods with data analysis techniques [10]. Decision theory plays a vital role in supporting threat-hunting activities. It analyzes the available intelligence and provides the hunters the most appropriate course of action based on their goals, preferences, and uncertainties.

## 2.5 Discussion – Novelty of Perspective

This study provides a novel perspective on the use of decision theory in addressing cyber threats. Decision theory serves as a powerful tool that empowers organizations with informed choices on allocating their cybersecurity resources. It unites data from various sources, enabling the decision-makers to quickly respond to threats make effective decisions based on the likelihood and impact of various cyber threats. This enables the organizations can make better decisions about which security measures to implement and how to prioritize their threat hunting activities. Through a comprehensive examination of normative, descriptive and prescriptive perspectives of decision theory, its significance across various domains of

cybersecurity such as risk assessment, intrusion detection, cybersecurity investment, threat hunting, zero trust architecture and AI-driven threat detection are illustrated. They novelty of this study lies in its thorough and organized exploration of the use of decision theory in CTI operations. It provides valuable insights into how decision theory can assist organizations in making informed and strategic decisions regarding CTI.

## 3. Current Trends

### 3.1 CTI Framework

CTI Framework typically consists of various processes, tools, and methods, it is a conceptual model that aids organizations to organize and apply threat intelligence to their cyber security operations. Any typical CTI Framework follows a certain process which as a result, produces output. It is also known as the intelligence cycle or CTI process. The intelligence cycle involves several stages: direction and planning, collection, processing and exploitation, analysis and production, and dissemination and integration.

1. **Direction and Planning** – In the direction and planning phase the organization establishes clear objectives and goals of the intelligence process.

2. **Collection** - In the collection phase the organization gathers relevant data. For the collection of raw data traditional intelligence uses techniques like open-source intelligence (ONSIT), human intelligence (HUMINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT) [10].

3. **Processing and Exploitation** – After gathering the necessary information, it progresses to a crucial stage called processing and exploitation. Here the raw data is transformed into meaningful information.

4. **Analysis and Production** – During this phase the data is carefully analyzed and the potential threats are evaluated. The final result is delivered to the intelligence users.

5. **Dissemination and Integration** – This phase involves the dissemination of analyzed intelligence and integrating it into existing security processes.

6. **Feedback** – In the final stage of CTI process, stakeholders provide feedback to evaluate the effectiveness and outcomes of the CTI activity. The intelligent cycle is depicted in the figure.1 below

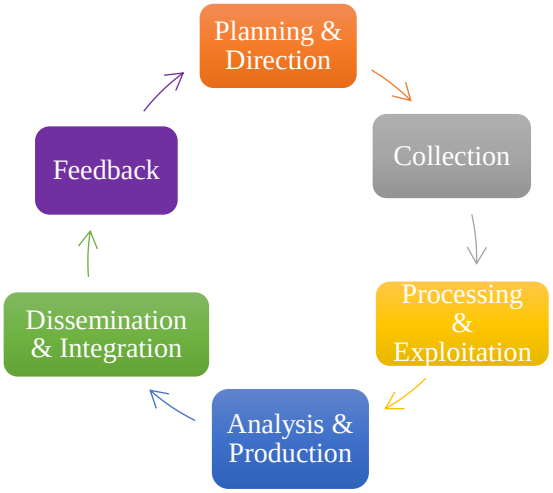


**Figure 1.** Intelligence Cycle

The following table.2 presents a comparative analysis of various existing CTI Frameworks based on their objectives, processes and usage. These frameworks show the diverse approaches organizations can adopt to carry out their CTI operations. The existing CTI frameworks provide powerful approaches for mitigating cyber threats. The assimilation of normative, descriptive, and prescriptive perspectives of Decision theory can provide a structured framework for making rational choices at every stage of the intelligence cycle.

**Table 2.** Comparative Analysis of Existing CTI Frameworks [12]

| Framework Name | Objective | Process | Usage |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Framework of Cyber Attack Attribution Based on Threat Intelligence | Trends of CTI | • Start Analysis<br>• Threat Intelligence<br>• Attribution Analysis | Introduce the methods and elements of threat intelligence-based component of cyber-attack attribution. |
| CTI Framework | To improve the understanding of the concept of CTI by presenting a much-needed definition of CTI and construct a model of the intelligence creation process | Data Processing Methods | CTI Framework /CTI Structure |
| New Intelligence Lifecycle[12] | Improve data quality through data evaluation; Enhance cyber-attack attribution | • Intelligence Lifecycle aggregation process | The proposed model and the definition aim to bring clarity on CTI from an enterprise perspective. |
| An Enhancement of Cyber Threat Intelligence Framework [12] | To address the challenges of gathering CTI data from multiple sources and creating analytics to shorten threat mitigation time.<br><br>To enhance CTI in terms of collection, filtering, sharing, visualization, and analysis. | • Direction and Planning<br>• Data Collection<br>• Data Analysis<br>• Sharing and Visualization | Identify threat actors through threat attribution; Share and visualize CTI information |
| Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data [13] | To analyze the lifecycle of cyber attackers and achieve attack goals in the pre- and post-attack exploit operational stages. | • Management<br>• Indexer<br>• Collect<br>• Generate<br>• Search<br>• Share<br>• Visualization<br>• Analysis | The proposed framework facilitates the collection, filtering, sharing, visualization, and analysis thereby improving threat comprehension and expediting mitigation efforts. |

| | | | |
|---|---|---|---|
| Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix [14] | To reduce the burden of human experts by leveraging Machine Learning techniques to enable automated validation of alerts. | • Identify problem and motivate<br>• Define Objectives<br>• Design and Development<br>• Demonstration and Evaluation | MITRE framework serves as a standalone resource for understanding and categorizing the tactics, techniques and procedures (TTPs) employed by cyber adversaries |
| A Framework for Automatic Identification and Classification of Cyber Threat Data [15] | | • Data Collection<br>• Send data to detector<br>• Generate alerts for suspicious activities<br>• Alert Validation using CTI<br>• Deliver validated data to security tool and teams. | Automate the process of validation of security alerts and incidents utilizing AI-based techniques. |

### 3.2 Existing Decision-Making Approaches and Methodologies

The integration of decision theory and cyber threat intelligence (CTI) is a promising area of research with the potential to revolutionize the way organizations make decisions. In this section The overview of the existing decision-making approaches and methodologies in Cyber Threat Intelligence (CTI) are presented.

#### 3.2.1 Decision Making Approaches in CTI

- **Traditional Approaches** Traditional approaches are based on the intelligence cycle, which is the process of collection, analysis, dissemination and consuming intelligence. These decision-making approaches in CTI involve analysts manually reviewing and analyzing the threat intelligence data to identify threats and assess them.

- **Data-Driven Approaches** Data-driven approaches use machine learning and AI to identify the patterns in intelligence data. Furthermore, machine learning algorithms can automate tasks such as data cleaning and analysis, enabling analysts to swiftly detect and prioritize threats.

#### 3.2.2 Decision Making Methodologies in CTI

The following table.3 gives a summary of the methodologies and tools employed in the CTI field to enhance decision making processes. These tools can be utilized individually or, in conjunction to enhance the decision-making process, for threat intelligence.

**Table 3.** Decision Making Methodologies and Tools in Cyber Threat Intelligence

| Methodology/ Tools | Usage | Benefits |
|---|---|---|
| Multi-Criteria Decision Making (MCDM) | Takes into account multiple criteria and preferences and helps to choose the best alternatives or choices. | Prioritization of security measures, resource allocation and risk management. |
| Indicator- Based Decision Making | Relies on Indicators of Compromise (IoCs) such as IP addresses, file hashes or URLs to identify and respond to cyber threats. | Accurate threat detection and response. |
| Decision Support Systems | Gathers and processes data from various sources such as security logs, threat intelligence field to provide actionable information. | Improved incident response, risk mitigation. |
| Risk Assessment Frameworks | Provide structured methodologies for assessment and management of cybersecurity risks, ensuring that organizations can identify vulnerabilities and allocate resources effectively. | Risk quantification, informed decision making, resource allocation. |
| Kill Chain Framework | Used to model and understand the stages of a cyber-attack, from initial reconnaissance to data exfiltration. | Allows early detection and mitigation of cyber threats. |
| Security Information and Event Management | Uses SIEM tools to collect, correlate and analyze security event data. | Real-time monitoring, centralized data management. |
| Machine Learning and Artificial Intelligence (AI) | Algorithms like classification and anomaly detection can be utilized in to identify malwares, network anomalies, and phishing emails. | Continuous threat monitoring, adapts well to evolving threats. |

### 3.3 Decision Theoretic Models for CTI

#### 3.3.1 Game Theory

Game theory provides a structured approach for understanding the interactions and conflicts that occur among agents with different preferences and goals. It also provides strategies to achieve those goals. By modelling the rational behaviour of these agents, game theory can help to identify and mitigate potential cybersecurity risks and threats. For example, consider a situation where multiple cloud service providers (CSP) operating within the same cloud computing environment are faced with the decision of whether to share information about cyber threats or keep it confidential. This scenario resembles a strategic game, with each CSP acting as a player whose choices impact the security of the overall cloud environment. The use of game theory allows for determining the best times for sharing information among them [16].

### 3.3.2 Fuzzy Logic

Fuzzy logic is a useful technique in handling variables, as it allows for the consideration of multiple possible truth values. Instead of being limited to simple binary distinctions like true/false or good/bad, fuzzy logic enables decision-making that takes into account more nuanced and flexible considerations. This is particularly helpful when dealing with cyber threats that don't neatly fit into clear categories [7]. Fuzzy logic introduces a nuanced approach to anomaly detection. For example, when monitoring the user login behaviour, traditional methods classify logins as either “normal” or suspicious”. In contrast, fuzzy logic assesses suspicion on a continuum, taking into account factors like login frequency, timing and device used. This allows more for precise detection of anomalies, assigning values like “slightly suspicious” or “moderately suspicious” to each login attempt [17].

### 3.3.3 Bayesian Networks

A Bayesian Network is a powerful tool in cyber security that uses probability to assess the likelihood of events. It is a graphical model that has gained widespread popularity due to its ability to overcome data limitations. Unlike other techniques, Bayesian Networks can handle uncertain and noisy data, reducing false positives and false negatives. By incorporating both existing information and probabilistic inferences, analysts can effectively evaluate and predict potential threats using Bayesian networks [12]. Bayesian networks are often used in Intrusion Detection Systems (IDS) because of their ability to handle uncertain and noisy data. IDS gather extensive data from various sources like traffic logs, system logs, and security events, which is often noisy and uncertain. This poses a challenge when detecting malicious activity using

conventional means. To overcome this challenge, IDS utilize Bayesian Networks to model the connections between different events within a network. By calculating the probability that an event is malicious, IDS can identify patterns of activity that may indicate an attack and promptly alert the security team for necessary actions.

### 3.3.4 Prospect Theory

Prospect Theory explains how individuals and organizations make choices when facing gains and losses. It suggests that people assess cybersecurity options based on deviations from their current security status. When there is a possibility for gains, individuals tend to be risk-averse, while they are more inclined to take risks in situations where losses are at stake. The way outcomes are presented and the individual's sensitivity toward gains and losses greatly impact decision-making processes [18]. For example, consider a scenario where a security analyst is responsible for securing confidential information from cyber threats. The analyst has two options: option A involves implementing an expensive but robust firewall that significantly reduces the risk of data breach, while option B entails no action, relying on existing security measures, potentially saving costs but carries higher data breach risk. Prospect theory plays a role here as the analyst leans towards option A, primarily driven by the principle of loss aversion [18].

## 4. Future Challenges

As the fusion of Decision Theory and CTI, is explored in the study it is important to understand the challenges that can arise. In this section, a closer look at challenges in the integration of Decision Theory in the development of CTI is presented.

### Complex and Dynamic Environments

The cyber-security field is always changing and bringing forth new and complex challenges. Traditional decision-making models may encounter difficulties in keeping pace with the fast-evolving and complex nature of these cyber threats. To overcome this challenge decision theory models that can handle the intricate nature of cyber threats and offer intelligent solutions must be developed.

### Ethical Considerations

Decision Theory assumes a rational decision-making process by overlooking ethical considerations. In CTI the decisions extend beyond their impact on technology outcomes, they also have ethical implications like user privacy, data security, etc. Integrating ethics into Decision Theory frameworks requires a thoughtful approach to ensure a holistic perspective.

### Data Quality and Uncertainty

The strength of Decision Theory rests on having accurate and reliable data. In CTI, uncertainties arise due to the difficulty of obtaining complete and trustworthy and timely threat details. When dealing with fuzzy or incomplete data can compromise the effectiveness of the decision model leading to inaccurate risk assessments.

### Scalability and Implementation

Scalability and practical implementation present major challenges as the CTI systems get more complex and data-intensive. Decision theory models that operate in small-scale situations could find it difficult to scale up to the demands of large-scale cyber threat environments. To overcome this, it is crucial to explore techniques for enhancing decision models through the utilization of machine learning, parallel processing, and distributed computing.

### Human Factors

Human biases and cognitive limitations can impact the decision-making processes. However, this challenge can be effectively tackled through the utilization of CTI, which involves the creation of decision aids that consider these biases and provide clearer and more comprehensible threat information to decision-makers.

## 5. Conclusion

This study provides a novelperspectives on the impact of decision theory on accumulating the finer aspects of cyber threat. Cyber threats can be sensed intelligently from decision theory models which include elements of adversarial reasoning and their behaviour. It is a research direction where the amount of effort to develop a cyber threat intelligence is

directly proportional to the amount of data collected from the behaviour of the cyber attackers. Even though development of a framework related to cyber threat takes fair amount of time, the adaptive intelligence propels the framework in the long run. The fusion of decision theory, including its normative, descriptive, and prescriptive standpoints, indicates a notable development in CTI. The study sincerely attempts to bring the robust correlation between the entities connected to decision theory which will be very much helpful to the designers of the cyber threat intelligence framework.

## References

[1] Abu, Md Sahrom, et al. "Cyber threat intelligence–issue and challenges." *Indonesian Journal of Electrical Engineering and Computer Science* 10.1 (2018): 371-379.

[2] Shin, Bongsik, and Paul Benjamin Lowry. "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished." *Computers & Security* 92 (2020): 101761.

[3] Aldauiji, Fatimah, Omar Batarfi, and Manal Bayousef. "Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art." *IEEE Access* 10 (2022): 61695-61706.

[4] Brown, Rebekah, and Pasquale Stirparo. "SANS 2022 cyber threat intelligence survey." *SANS, Feb* 23 (2022).

[5] Ainslie, Scott, et al. "Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice." *Computers & Security* (2023): 103352.

[6] M'manga, Andrew. *Designing for cyber security risk-based decision making*. Diss. Bournemouth University, 2020.

[7] de Gusmão, Ana Paula Henriques, et al. "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory." *International Journal of Information Management* 43 (2018): 248-260.

[8] Xiao, Liyuan, Yetian Chen, and Carl K. Chang. "Bayesian model averaging of Bayesian network classifiers for intrusion detection." *2014 IEEE 38th International Computer Software and Applications Conference Workshops*. IEEE, 2014.

[9] Fielder, Andrew, et al. "Risk assessment uncertainties in cybersecurity investments." *Games* 9.2 (2018): 34.

[10] Nagurney, Anna, and Ladimer S. Nagurney. "A game theory model of cybersecurity investments with information asymmetry." *NETNOMICS: Economic Research and Electronic Networking* 16 (2015): 127-148.

[11] Groš, Stjepan. "Research Directions in Cyber Threat Intelligence." *arXiv preprint arXiv:2001.06616* (2020).

[12] Abu, Sahrom, et al. "An enhancement of cyber threat intelligence framework." *J. Adv. Res. Dyn. Control. Syst* 10 (2018): 96-104.

[13] Borges Amaro, Lucas José, et al. "Methodological framework to collect, process, analyze and visualize cyber threat intelligence data." *Applied Sciences* 12.3 (2022): 1205.

[14] Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. "Assessing mitre att&ck risk using a cyber-security culture framework." *Sensors* 21.9 (2021): 3267.

[15] Islam, Chadni, et al. "SmartValidator: A framework for automatic identification and classification of cyber threat data." *Journal of Network and Computer Applications* 202 (2022): 103370.

[16] Amini, Mahyar, and Zavareh Bozorgasl. "A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology." *International Journal of Computer Science and Engineering Research* 11.4-2023 (2023).

[17] de Campos Souza, Paulo Vitor, et al. "Detection of anomalies in large-scale cyberattacks using fuzzy neural networks." *AI* 1.1 (2020): 5.

[18] Qu, Leilei, et al. "Towards better security decisions: applying prospect theory to cybersecurity." *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 2019.