
STRATEGIC CYBER DECISION-MAKING UNDER EVOLVING INTELLIGENCE: A DYNAMIC BAYESIAN GAME-THEORETIC FRAMEWORK FOR AI-ASSISTED CYBER THREAT INTELLIGENCE

Zohaib Gillani

Adjunct Faculty

*Department of Defence & Strategic Studies,
Quaid-i-Azam University, Islamabad*

Zohaib.gillani@asc.qau.edu.pk

Zahid Mehmood Zahid

Assistant Professor

*Department of Strategic Studies
Air University Islamabad, Pakistan*

zahid.mehmood@au.edu.pk

ABSTRACT

Artificial Intelligence (AI) is revolutionizing Cyber Threat Intelligence (CTI), facilitating quicker detection, analysis, and response to cyber threats with enhanced precision. But current studies on AI for CTI tend to focus exclusively on the engineering side of the problem, with a scope that includes threat detection, malware classification, anomaly detection and automated response, rather than the strategic aspects of information-gathering that takes place between adaptive attackers and defenders when information is incomplete. This research introduces a Dynamic Bayesian Game-Theoretic Framework that combines AI-assisted CTI with strategic decision-making in the presence of uncertainty. The proposed framework differs from traditional cyber security game models, which consider information as exogenous and fixed, by treating the quality of intelligence as an endogenous game variable, which is continuously evolving. In the face of ever-evolving attacks and counterattacks, defender beliefs are dynamically updated by Bayesian learning using AI-generated cyber intelligence, and attackers dynamically change their behavior based on defenders' actions, leading to strategic equilibrium evolving over repeated interactions. It embeds all these essential components of rational attacker-defender interaction, incomplete information, dynamic belief updating and AI supported intelligence generation within a single analytical model. The 2021 Colonial Pipeline ransomware attack is used to demonstrate how AI-driven CTI can increase situational awareness, speed up Bayesian belief updating, aid in defense decision-making, and minimize

strategic uncertainty during ransomware attacks. This study adds value by incorporating AI-based CTI into DBGTT, by making cyber intelligence more dynamic than a given information assumption, and by offering an analytical basis for adaptive cyber defense and critical infrastructure security via AI-driven intelligence.

KEYWORDS

Artificial Intelligence, Cyber Threat Intelligence, Dynamic Bayesian Game Theory, Strategic Decision-Making, Cyber security, Critical Infrastructure, Colonial Pipeline, Bayesian Learning.

INTRODUCTION

Governments, critical infrastructure, financial systems, healthcare systems, and industrial control systems are increasingly relying on digital technologies, making cyberspace a pivotal arena with the potential for economic, political, and national security impact from cyber-attacks. The Colonial Pipeline ransomware attack, the Solar Winds supply-chain incident and cyber operations targeting critical infrastructure in interstate conflicts are just some examples of recent events that illustrate that today's cyber-attacks are as much an act of strategy as they are a technical event, requiring smart adversaries, asymmetric information, and continual adaptation. However, with the rise in complexity of cyber-attacks, the signature-based and rule-based methods have proven unable to defend against advanced persistent threats, ransomware, zero-day vulnerabilities or AI-supported attack methods. As a result, organizations have moved away from a reactive to an intelligence-driven approach that is able to predict adversarial activities before they happen (Buczak & Guven, 2016; Manshaei et al., 2013).

An integral element to this shift is Cyber Threat Intelligence (CTI), which is aimed to take a diverse and complex cyber data and create actionable intelligence that can complement proactive defense. While Indicators of Compromise (IoCs) are important, CTI is more than that, combining technical, operational, and contextual data about the threat actors, vulnerabilities, attack campaigns, and adversarial tactics to enhance situational awareness and decision making. The recent systematic review reports show that AI technologies such as machine learning, natural language processing, and knowledge representation have significantly contributed to the enhancement of CTI through faster identification, correlation, and detection of anomalies and predictive capabilities. However, they also feel that there are still a lot of challenges ahead such as quality of intelligence, interoperability, trust, and assimilation of generated intelligence in operational decisions.

Although much of the literature in the field of AI and CTI has concentrated on the technical aspect of enhanced performance, Cyber security is a strategic problem where decisions are made by both an adaptive attacker and defender, and the information is incomplete and evolving over time. Simultaneously, game theory has emerged as one of the major tools to model cyber conflict, as it clearly accounts for uncertainty and rational decision-making as well as strategic interaction. There have been several previous studies that were able to solve cyber security issues like intrusion detection, resource allocation, cyber insurance, and network defense using static games, Stackelberg games, Bayesian games, and deception games (Manshaei et al., 2013; Do et al., 2017). These models, however, tend to assume that defenders know what entities they can use in their strategy or that they are given a set of entities to use. They are unlikely to think that today's SOC's constantly produce new intelligence using AI-powered CTI, which changes defender's beliefs throughout the duration of a cyber campaign.

This divide is a theoretical gap that is significant. Current AI-based CTI research can be used to understand the genesis of intelligence, while game-theory-based research in cybersecurity can be used to understand rational actors' behavior when information is incomplete. There is comparatively little research that combines these aspects to understand how AI-generated intelligence impacts Bayesian beliefs, strategic decision making, and the resulting behavior when the attacker–defender interaction is repeated. Existing models thus only partially explain decision-making in an AI-supported cyber environment, where intelligence evolves dynamically and affects the future behavior of the decision. Therefore, the existing models can only explain decision-making to a certain extent, as in the AI-supported cyber environment, intelligence itself changes dynamically and shapes the future behavior of the decision.

To fill this void, this study introduces a Dynamic Bayesian Game-Theoretic Framework for AI-assisted Cyber Threat Intelligence that can be used to model the behavior of cyber adversaries. To fill this void, this study proposes a Dynamic Bayesian Game-Theoretic Framework for AI-assisted Cyber Threat Intelligence for modelling cyber adversarial behavior. The framework assumes a cyber conflict as a repeated interaction of a rational attacker and defender operating under incomplete information and where defender beliefs are continuously updated based on acquired cyber intelligence that are generated by AI. The proposed framework is different from the traditional Bayesian cybersecurity models, where intelligence is an exogenous factor that affects the cost-effectiveness of information. In the proposed model, the strategic evolution of AI-supported cyber intelligence is considered as an endogenous factor that can shape the nature of the information, influence the strategic adaptation of actors, and lead to different equilibrium outcomes over time.

The ability of the proposed framework to be used in analysis is demonstrated by one of the most impactful cyber incidents impacting critical infrastructure in recent years, the Colonial Pipeline ransomware attack (2021). The case is not statistical proof but rather illustrates the potential of continuously generating intelligence using AI to validate belief updating in Bayesian belief systems, enhance situational awareness, and enable a more adaptive defensive decision-making process in a ransomware attack. This work brings the fields of cybersecurity and decision-science together in one analytical framework to model strategic cyber decision-making in the presence of dynamic information conditions and extends the literature by adding the modelling capabilities of AI-assisted CTI.

LITERATURE REVIEW

Artificial Intelligence-Assisted Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is no longer a reactive security effort focused on an IOC, but a strategic capability that assists proactive cyber defense by gathering, analysing, and sharing actionable intelligence. CTI brings together the technical, operational, and strategic intelligence related to adversaries, vulnerabilities, infrastructure, and attack campaigns to enhance the decision-making process within the organization, while traditional intrusion detection systems focus on the detection of known attack signatures. With the rise in sophistication of ransomware, advanced persistent threats, and state sponsored cyber campaigns, CTI has become an integral part of the cybersecurity resilience equation (Hutchins, Cloppert, & Amin, 2011; Mavroeidis & Bromander, 2021).

Artificial Intelligence (AI) developments have significantly increased the analytical power of CTI systems in recent years. Machine learning algorithms can be used to automatically detect anomalies and classify malware, and natural language processing can be used to extract threat intelligence from unstructured reports, vulnerability disclosures, and open-source intelligence. More recently, knowledge graphs and large language models have enhanced the way analysts understand relationships between threat actors, tactics, techniques, and procedures (TTPs) and vulnerabilities, allowing for the creation of more meaningful and timely intelligence than traditional rule-based systems. As such, AI has taken the place of the traditionally descriptive approach to CTI to become a dynamic decision-making support tool that continuously processes the vast diversity of cyber information for more effective situational awareness (Buczak & Guven, 2016; Mavroeidis & Bromander, 2021).

However, with all these progressions, there are also certain drawbacks identified in literature. Current AI-driven CTI systems are susceptible to adversarial

manipulation, limited explainability, data quality problems, false positives, and model drift. In addition, most of the studies evaluate the performance of AI based on engineering-based metrics like accuracy in detection, precision, recall, or processing speed. While these are examples of technical enhancements, they offer relatively limited understanding of the impact of AI-enabled intelligence on strategic interaction between adaptive attackers and defenders. In the real world of operations, intelligence is not just a product of analytical systems, but a strategic asset to inform future actions and influence adversarial actions. This strategic dimension is relatively underdeveloped in the literature that focuses on the use of AI in CTI (Santos et al., 2025).

In this way, the surge of artificial intelligence not only affects the pace of the creation of intelligence, but also the context in which cyber decisions are made. These constant updates to defender knowledge of attacker behavior, along with the continuous adjustments made by the attackers to evade detection, to alter observations, or to exploit weaknesses in AI models, are all occurring in real time. As a result, processes of intelligence generation and strategic adaptation become synergistic. The analytical frameworks that capture this interaction must be able to model belief and uncertainty evolution, as well as repeated strategic decision making, and not only rely on computational performance metrics to assess the performance of AI.

Game-Theoretic Models in Cybersecurity

As cyber threats evolve and become more sophisticated, strategic decision-making in cybersecurity has grown in importance. In contrast to engineering challenges, in cyber conflict, both the attackers and the defenders are smart and continuously adapt their behaviour to the other. The attacker wants to increase the likelihood of compromising the systems and decrease the chances of being detected while the defender wants to spend limited resources on systems to increase their resilience and decrease the chance of discovering he or she has been compromised. Cybersecurity has come to be an important application domain of game theory because the success of either party not only relies on their own decision but also on what they expect their rival to do (Manshaei et al., 2013).

Game theory offers a mathematical tool to study strategic interaction in situations of competition, uncertainty, and interdependence. Initial uses of cybersecurity were based on static games, in which both the attacker and defender gathered their strategies at a fixed time, based on a given payoff function. These models were found to be useful to analyses the issues of intrusion detection, vulnerability management, and optimal resource allocation as they yielded analytic tractable equilibrium solutions. But their assumptions of fully observed information and one-stage interaction had the effect of restricting their usefulness in operational

cyber environments where attackers are often able to hide capabilities, change tactics and simply exploit unknown vulnerabilities (Manshaei et al., 2013).

To better model sequential decisions, researchers employed "Stackelberg Security Games (SSGs)" that assumed that the defenders would make a security decision in advance of the attackers. The Stackelberg models have been extensively used in network defense, moving target defense, cyber deception, and critical infrastructure protection since they formally model the strategic anticipation of the opposing players. However, the typical models assume a rather fixed information structure and given leader–follower relationships. Neither defenders nor attackers know all that much about the other's capabilities, technology or goals, and both parties are constantly monitoring and adapting to each other's actions. Thus, the uncertainty of today's cyber operations is only partially represented in a Stackelberg formulation (Do et al., 2017).

The limitations have led to the use of the Bayesian approach to modeling strategic interaction in the presence of incomplete information. In Bayesian games, decision makers are uncertain about the characteristics or intentions of their opponents and thus make decisions based on a belief, rather than a fact. In the field of cybersecurity, Bayesian models are utilized in intrusion detection, cyber insurance, access control, vulnerability disclosure and attack attribution scenarios to better capture the uncertainty associated with the type of attacker and the attacker's capabilities of defense (Harsanyi, 1967, 1968; Manshaei et al., 2013). The framework of Bayesian games offers a more practical approach to cyber conflict modelling than the traditional static approach because of its features of belief updating and strategic decision-making.

While these are some of the methodological advances, the current game-theoretic cybersecurity models typically assume information as an exogenous input. While Bayesian beliefs could evolve because of observing attacker behavior this is not always the case for intelligence itself. Today's cyber defense, however, is built on (AI-driven) Cyber Threat Intelligence, which uses machine learning to automatically process a series of data streams (network telemetry, threat intelligence feeds, behavioral indicators, vulnerability information) and turn them into new intelligence, as part of an ongoing cyber campaign. Defenders gain more intelligence, and their ideas of what the attackers can do and want to do change as well, while attackers try to change their behavior to maintain their strategic edge. As a result, cyber conflict is no longer linear, in the sense that intelligence is gathered and then used to adapt strategy but is a process whereby intelligence is generated and strategy is adapted, all at once.

As this observation shows, there are quite a few gaps in the literature. Existing game-theoretic models can explain strategic interaction in uncertain environments

but have limited ability to explain the time evolution of belief formation and equilibrium behavior due to the presence of AI-generated intelligence. There is a lack of analytical integration of AI-assisted CTI with Bayesian strategic reasoning, however. This restriction needs to be overcome by putting intelligence generation on the strategic agenda as an integral part of the decision-making process instead of an external assumption. This is the conceptual framework for the Dynamic Bayesian Game-Theoretic Framework suggested in this study.

Research Gap and Conceptual Positioning

The foregoing review confirms that the field of cybersecurity research has made huge strides in the past few years in both upon the use of artificial intelligence in cyber threat intelligence (CTI) and game-theoretic modelling of cyber conflict. AI models have greatly contributed to the fields of threat detection, anomaly detection, malware classification, intelligence fusion and predictive cyber analytics, and game-theoretic models have helped shape understanding of strategic interaction between attackers and defenders in situations of uncertainty (Buczak & Guven, 2016; Mavroeidis & Bromander, 2021; Manshaei et al., 2013; Do et al., 2017). All of these have contributed to the technical and strategic arms of cybersecurity, overall. However, they are not well integrated as an analytical approach and have developed as parallel research strands.

Existing AI-assisted CTI research tends to focus on the performance metrics associated with the CTI system, such as engineering-based metrics like detection accuracy, precision, recall, false-positive rate, computational efficiency, and response latency. These studies have significantly enhanced the efficiency of the current SOC's and helped to identify the threats quickly and process them better. They offer, however, rather less analysis of the impact of AI-driven intelligence on the strategic decision-making process during cyber conflict. Typically, intelligence is considered as a product of an analytical system and not as a strategic factor which continually influences attackers and defenders' behavior (Mavroeidis & Bromander, 2021; Santos et al., 2025).

On the other hand, the interaction between the attacker and the defender has been successfully modelled using static, Stackelberg, Bayesian, stochastic and repeated games in the domain of cybersecurity. In contrast, the interaction between the attacker and defender has been successfully modelled in the context of cybersecurity using static, Stackelberg, Bayesian, stochastic, and repeat games. Such models have been used in various applications such as intrusion detection, cyber deception, resource allocation, access control, and critical infrastructure protection (Manshaei et al., 2013; Do et al., 2017). However, most of the current models make two assumptions: first that the information accessible to decision makers is fixed, and second that the information is updated by a series of pre-

programmed probabilistic observations. They do not often realize that in modern cyberspace, intelligence has constantly evolved due to AI-powered threat analysis, behavioral learning, and intelligence fusion.

One theoretical constraint of this separation between the generation of intelligence through AI and strategic decision-making. Attacks constantly change their methods to avoid detection, and defenders are always seeking to gain more insight into their environment using AI-powered Cyber Threat Intelligence. In an operational cyber environment, attackers are perpetually trying to change their tactics to evade detection, and defenders are continuously working to gain more insight in their environment using AI-powered Cyber Threat Intelligence. As a result, the quality of information gathered and the decision makers' strategic interpretations, which form the basis for the decisions they make, change during the interaction process. There is limited existing research that explains how these two processes interact, within a single analytical approach.

To overcome this, the present study suggests using an endogenous approach to strategic interactions by incorporating an AI-driven Cyber Threat Intelligence as an internal game component instead of an external source of information. This framework assumes that AI systems will continually produce new insights into the cyber space, modify the defender's beliefs using Bayesian learning, and then drive strategic choices. Meanwhile, the attackers watch the defenders' reactions and will adjust their own tactics, and so on—and on it goes, learning, adapting, revising beliefs. Unlike models that analyze the intelligence process and the strategic process separately, the proposed framework is more realistic in representing the decision-making process in modern cyber conflict as it is a combination of AI-driven intelligence generation and Bayesian strategic logic.

For this reason, the results of this study make a significant contribution to literature in three main aspects. First, it unifies the three major disciplines of Artificial Intelligence, Cyber Threat Intelligence, and Dynamic Bayesian Game Theory, into one analytical framework of cyber decision-making. Second, it regards the information that AI generates as a strategic variable that is constantly changing and altering information asymmetries and the behavior of equilibrium. Finally, it provides a concrete example of how the proposed framework can be applied in a real-world scenario, such as the Colonial Pipeline ransomware attack, which could be used to enhance the effectiveness of defensive strategies and resilience against ransomware threats in the protection of critical infrastructure. This is the mathematical formalism of these contributions, which is developed in the following section.

PROPOSED DYNAMIC BAYESIAN GAME-THEORETIC FRAMEWORK

Model Structure and Assumptions

This study introduces a Dynamic Bayesian Game-Theoretic Framework that combines Artificial Intelligence-assisted Cyber Threat Intelligence (CTI) and repeated gameplay between an attacker and a defender to analyse strategic cyber decision-making under evolving intelligence conditions. The framework follows standard Bayesian cyber security games, but with the twist that the information sources used are derived from AI-generated intelligence and not from an outside source. Defender beliefs constantly change with AI's new knowledge of cyber, while attackers continually adjust their tactics to maintain effectiveness.

The model assumes the presence of two rational players:

Attacker (A): an individual or organization that tries to achieve the greatest possible probability of achieving a positive outcome from a cyber-attack while minimizing the chances of defensive countermeasures being misapplied.

Defender (D): a security organization that uses AI assisted CTI to identify threats, refresh its intelligence, and reduce the likelihood of an operation losing a significant amount of business.

There is incomplete information for both players. Initially, neither the defender nor the attacker knows the full extent of their capabilities, resources, or intent, and the attacker only has partial information about the defender's ability to monitor, his (or her) AI maturity, and his (or her) effectiveness in responding. In situations where strategic decisions must be made with incomplete information, their decision making follows the paradigm of the Bayesian game theory (Harsanyi, 1967, 1968).

The idea of the proposed model differs from the traditional Bayesian frameworks for cybersecurity in that the intelligence is learning during the interaction process. The AI continuously scans network telemetry, behavioral metrics, threat intelligence feeds, malware signatures, and past attack data to create new cyber intelligence. The observations change defender beliefs about the attacker behavior, which in turn affects selection of defense strategies. Meanwhile, defenders are watching for reactions and are adjusting their defensive strategies and tactics by changing attack vectors, timing, defensive infrastructure, etc., or modifying the attack itself. The interaction process is thus a cycle of observation, learning, adaptation, and strategic optimization.

To simplify analysis, the model is constructed based on the following assumptions:

- 1. Rationality:** Player on both sides maximizes expected utility, based on their information.

2. **Incomplete Information:** No player has all the information about the opponent's traits or behavior.
3. **Dynamic Intelligence:** AI-assisted CTI creates new intelligence throughout the interaction, which updates defender beliefs.
4. **Bayesian Learning:** Strategic beliefs are updated sequentially considering the observed cyber events following the Bayes Rule.
5. **Repeated Interaction:** Cyber conflict is a dynamic process, not a one-shot game.
6. **Adaptive Behavior:** Both players adapt their strategies to new intelligence.

The assumptions enable the proposed framework to model modern cyber warfare more accurately than static or one-shot game-theoretic models, in which the intelligence of actors is assumed to remain constant during the game of interaction.

The principal variables are defined for the formalization of the model in Table 1.

Symbol Definition

- (A) Attacker
- (D) Defender
- (θ) Attacker type (capability or sophistication)
- (S_A) Attacker strategy
- (S_D) Defender strategy
- (I_t) AI-generated cyber intelligence at time (t)
- (B_t) Defender belief at time (t)
- (U_A) Attacker utility
- (U_D) Defender utility
- ($P(\theta)$) Prior belief regarding attacker type
- ($P(\theta | I)$) Posterior belief after observing intelligence
- (L_t) AI learning process
- (E_t) Strategic equilibrium at time (t)

Overall analytical logic of the proposed framework shown in figure 1. AI-supported CTI is always generating intelligence because of the cyber events that are observed. This intelligence is used to update the beliefs of defenders using Bayesian learning and affect decisions of which defensive strategy to pursue. The attackers then watch the defensive activity and change their way of doing things, resulting in new observations that are fed back into the intelligence cycle. As a result, the generation of intelligence, the updating of beliefs and the adaptation to strategies become interdependent processes, which influence equilibrium behavior during repeated interactions.

Mathematical Formulation

The game between attacker and defender is modelled as a dynamic Bayesian game with two players making repeated decisions where they lack complete information. The defender's information set is continually modified with the use of Artificial Intelligence in Cyber Threat Intelligence (CTI) and beliefs about attacker behavior can be continually updated because of repeated interaction, unlike traditional Bayesian cybersecurity models.

The game is formally represented as

$$G = \langle N, \Theta, S, P, U, T \rangle$$

where

- $N = \{A, D\}$ denotes the set of players consisting of the attacker (A) and defender (D);
- $\Theta = \{\theta_A, \theta_D\}$ represents the private information (types) of each player.
- $S = \{S_A, S_D\}$ denotes the available strategy sets.
- $P(\Theta)$ represents the initial probability distribution over player types.
- $U = \{U_A, U_D\}$ denotes the utility functions.
- T represents repeated interaction across discrete decision periods.

The probability distribution is not assumed to be constant unlike the traditional Bayesian games. Rather, AI-powered CTI is constantly producing new intelligence that continually changes the defender's information set for every cyber event that it observes.

● ***Attacker Strategy***

The attacker selects one strategy from

$$S_A = \{Attack, Delay, Deceive, Withdraw\}$$

Where,

- **Attack** represents immediate cyber operation.
- **Delay** postpones offensive action while gathering intelligence.
- **Deceive** attempts to manipulate defender observations.
- **Withdraw** terminates the operation.

The selected strategy depends upon the attacker's expected probability of success and anticipated defensive response.

● ***Defender Strategy***

The defender chooses.

$$S_D = \{Monitor, Detect, Mitigate, Recover\}$$

Where,

- **Monitor** collects intelligence.
- **Detect** identifies malicious activity.
- **Mitigate** deploys defensive countermeasures.
- **Recover** restores system functionality following compromise.

Strategy selection depends upon the defender's current belief regarding attacker capability together with intelligence generated by AI-assisted CTI.

● ***Information Structure***

Let

$$I_t$$

denote the intelligence generated during decision period t .

Unlike previous cybersecurity game models,

$$I_t$$

is not constant.

Instead,

$$I_t = f(L_t, O_t)$$

where

- L_t denotes AI learning capability,
- O_t represents newly observed cyber events.

Consequently,

the quality of intelligence evolves after every interaction.

This constitutes the principal methodological innovation of the proposed framework.

● **Utility Functions**

The attacker seeks to maximize

$$U_A = B - C_A - D$$

Where,

- B denotes the expected operational benefit,
- C_A represents attack cost,
- D represents expected defensive losses imposed upon the attacker.

The defender seeks to maximize

$$U_D = R - C_D - L$$

Where,

- R denotes system resilience,
- C_D represents defensive expenditure,
- L represents expected cyber losses.

These straightforward utilities represent the strategic balance between operational value, resource investment, and anticipated risk. They also serve as a foundation for the derivation of equilibrium behavior in the following sections.

● *Dynamic Interaction*

The game proceeds through repeated stages.

At each decision period

1. The attacker selects a strategy.
2. A cyber event occurs.
3. AI-assisted CTI analyses the event.
4. New intelligence is generated.
5. Defender beliefs are updated.
6. The defender selects a response.
7. The attacker observes the response and revises future strategy.

The interaction continues until the attacker chooses to end the campaign or the defender can effectively neutralize the attack.

Thus, strategic behavior is a result of the ongoing co-evolution of the generation of intelligence, the updating of Bayesian belief, and the adaptation of decision making.

Bayesian Belief Updating with AI-Assisted Cyber Threat Intelligence

One of the hallmarks of modern cyber warfare is that defenders don't have a lot of firsthand information at their disposal. Rather, intelligence is constantly gathered by Artificial Intelligence that analyzes network telemetry, threat intelligence feeds, behavioral indicators, malware attributes, and external intelligence feeds. This means that defender perceptions of what the attackers can do and what they are going to do are adjusted during the interaction process, not at the end of the period of play. The proposed framework builds upon the classical Bayesian updating to incorporate AI-enabled Cyber Threat Intelligence (CTI) into the information set of the game to capture this property.

Let the type of the attacker be hidden and represent it by θ , $\theta \in \Theta$. Prior to observing a cyber event, the defender forms a belief $(P(\theta))$ about the likelihood the attacker is a member of a specific threat category. Based on this observation, the defender's belief about cyber intelligence I_t is updated using Bayes' rule:

$$P(\theta|I_t) = \frac{P(I_t | \theta) P(\theta)}{\sum_{\theta' \in \Theta} P(I_t | \theta') P(\theta')}$$

where $P(I_t|\theta)$ represents the likelihood of observing intelligence I_t given attacker type θ .

This formulation follows the standard Bayesian updating mechanism. However, unlike conventional cybersecurity game models, the quality of intelligence is not assumed to be fixed. Instead, AI continuously refines the evidence available to the defender through learning from newly observed cyber events.

To represent this process, the intelligence available at time t is defined as

$$I_t = \lambda_t O_t,$$

where O_t denotes observed cyber evidence and $\lambda_t \in [0,1]$ represents the AI intelligence quality coefficient. Higher values of λ_t indicate more reliable and informative intelligence generated through AI-assisted CTI, whereas lower values represent incomplete, noisy, or misleading observations resulting from limited visibility or adversarial manipulation.

The intelligence quality coefficient evolves over time according to

$$\lambda_{t+1} = \lambda_t + \alpha L_t - \beta A_t,$$

Where,

- α denotes the learning efficiency of the AI system.
- L_t represents knowledge gained from newly analyzed cyber events.
- β measures the impact of adversarial adaptation.
- A_t captures attacker actions intended to degrade or evade intelligence collection, such as deception, obfuscation, encrypted communications, or adversarial machine-learning techniques.

This formulation reflects the reality that AI does not automatically produce perfect intelligence. Instead, intelligence quality improves through learning but may deteriorate when attackers successfully manipulate or conceal observable information.

The posterior belief obtained from Bayesian updating directly influences the defender's strategic choice. As the AI system generates more reliable intelligence,

uncertainty concerning attacker capability decreases, enabling the defender to allocate resources more efficiently and reduce expected cyber losses. Conversely, when intelligence quality deteriorates because of deception or incomplete observations, posterior beliefs become less informative, increasing the likelihood of suboptimal defensive decisions. Strategic behaviour therefore depends not only on observed cyber events but also on the quality of intelligence extracted from those events.

Unlike existing Bayesian cybersecurity models that treat observations as externally determined, the proposed framework models AI-assisted intelligence generation as an endogenous process that continuously reshapes the defender's information set. Consequently, Bayesian beliefs, strategic decisions, and equilibrium behaviour co-evolve throughout repeated attacker-defender interaction. This integration of AI-assisted CTI with Bayesian learning constitutes the principal methodological contribution of the proposed framework and provides the analytical basis for the equilibrium analysis presented in the following subsection.

ILLUSTRATIVE APPLICATION OF THE PROPOSED FRAMEWORK: THE COLONIAL PIPELINE RANSOMWARE ATTACK

To illustrate the analytical potential of the Dynamic Bayesian Game-Theoretic Framework proposed in this study, the study simulates the Colonial Pipeline ransomware attack of May 2021. The attack is one of the most significant cyber incidents to target critical infrastructure in the United States, and is a good example of the effect of strategic uncertainty, incomplete information, and dynamic decision-making on cyber defense during ransomware attacks. The Colonial Pipeline incident is not intended to be a statistical example, but instead demonstrates how AI powered Cyber Threat Intelligence (CTI) can continuously update defender beliefs and enhance strategic responses in an ever-changing cyber operation (CISA, 2021; GAO, 2022).

Colonial Pipeline Co. has about 5,500 miles (8,850 km) of pipeline facilities that carry nearly 45% of the fuel used on the U.S. East Coast, ranging from gasoline to diesel fuel and jet fuel. The company was able to identify a ransomware attack on its corporate information technology (IT) network on 7 May 2021. While investigators did not find any evidence of specific compromise of the operational technology (OT) network running pipeline operations, Colonial Pipeline voluntarily halted fuel movement in order to minimize risk to operations and to enable incident response teams to evaluate risk to operational systems. The shutdown had a significant impact on fuel supply in several states, caused temporary shortages and panic buying, and prompted a federal emergency declaration stressing the importance of strategic cyber security for critical

infrastructure (CISA, 2021; U.S. Government Accountability Office [GAO], 2022).

The Federal Bureau of Investigation went on to place the blame on the ransomware-as-a-service (RaaS) group DarkSide, a financially motivated cybercrime group. The attacks are believed to have been made by exploiting a Virtual Private Network (VPN) account that was not being used and lacked multi-factor authentication. Once the attackers had infiltrated the corporate network, they exfiltrated some 100 GB of corporate data prior to deploying ransomware, doubling the pressure on the victim organization by adding data theft to ransomware. Colonial Pipeline ended up paying about 75 Bitcoin (or about \$4.4 million at the time) to get a decryptor, but post-recovery efforts were mostly based on the inside as the decryptor that was supplied ran slowly. Later, the U.S. Department of Justice recovered about 63.7 Bitcoin from the ransom payment as a result of law-enforcement efforts (FBI, 2021; DOJ, 2021; GAO, 2022).

The attack in the proposed Dynamic Bayesian setting starts from a partially-informative setting. The defender is initially only a person with preconceptions about who the attacker is and what they are capable of and what they might be trying to do. Once it is detected, there is doubt about the extent of the intrusion, that operational technology has been compromised, and if the attackers have other forms of persistence in the network. Therefore, decisions that must be made in defence, such as the suspension of pipeline operations, must be made before full information is available. This decision-making framework directly corresponds with the Bayesian assumptions reached in Section 3, where rational defenders maximize expected utility, given incomplete, but continually updated, intelligence.

AI-powered Cyber Threat Intelligence constantly collects new information from endpoint telemetry, network logs, forensic artefacts, malware analysis, external threat-intelligence feeds, and IOE/IOA exchanges with government agencies and private-sector partners as the incident unfolds. In the suggested model, these observations are used to improve the quality of the available intelligence, thus keeping the defender's posterior beliefs up to date regarding attacker capability and intent. Better intelligence gives them better information on which to base decisions on containment, system restore, forensic analysis, and national cybersecurity agencies. At the same time, attackers strive to maintain informational superiority by operating in stealth mode, executing an attack quickly, and deploying ransomware before defenders reach the correct level of intelligence. The interaction is a repeated strategic process in which generating intelligence and adversarial adaptation take place at the same time and not one after another.

This is the Colonial Pipeline incident to show that the benefits of AI-powered CTI go beyond technical detection. The strategic value is its ability to mitigate information asymmetry between attackers and defenders so that the updating of the Bayesian belief becomes more accurate and the allocation of resources more effective during cyber crisis. The current scenario example demonstrated in this framework can be applied to various types of cyber operations, including advanced persistent threats, supply-chain attacks, critical infrastructure protection, and state-sponsored cyber campaigns. In conclusion, the proposed Dynamic Bayesian framework provides a theoretically sound framework to analyze strategic cyber decision-making in cases where the intelligence evolves continuously during the attacker–defender interaction.

DISCUSSION

Results from this study indicate that integrating the AI-based Cyber Threat Intelligence (CTI) with Dynamic Bayesian Game Theory (DBGTT) offers a richer framework for analysis of strategic cyber decision-making than the use of these two fields separately. While previous research on AI for CTI has mainly targeted technical aspects, such as better threat detection, anomaly detection, malware classification, and intelligence automation, game-theoretic research has focused on modelling in the context of incomplete information. The proposed framework, by incorporating these views, considers cyber intelligence as a strategic asset rather than a mere operational information, constantly affecting the behaviour of attacker and defender.

The most significant theoretical value of the framework is to regard the intelligence that is generated through AI as an endogenous variable in the strategic decision-making process. Typical Bayesian cybersecurity models have a set of pre-defined observations followed by a belief update. The proposed framework, on the other hand, acknowledges that modern SOC's are continually producing new intelligence via machine learning, behavioral analytics, and intelligence fusion. This means that the information that the defender draws on is constantly updated during the interaction itself, so that Bayesian beliefs and strategic choices can evolve with the new data. This is a more realistic view of the operational challenges now faced by cyber defense, in which information quality evolves over the course of an incident, not at its beginning.

The example of the Colonial Pipeline ransomware incident illustrates how intelligence can change in response to a cyber incident and impact the decision-making process of defenders. The framework is not a predictor of what will happen during a particular attack, but a structured analytical analysis methodology for reviewing the interplay between intelligence generation, uncertainty and strategic adaptation over time. This could help cyber security

analysts in considering other defense options, allocate security resources in the face of uncertainty and increase organizational adaptability to adaptive adversaries.

The framework also, in practical terms, has implications for organizations that are responsible for protecting critical infrastructure. AI assisted CTI must be considered as more than just a tool for boosting detection accuracy, but as a strategic decision support capability. The use of AI-generated intelligence in formal decision-making could help security teams mitigate information asymmetry, prioritize defensive measures, and be more effective in responding to rapidly changing cyber threats. Moreover, the framework can be used to enable cyber security training, incident response planning, cyber risk assessment, and decision support in Security Operations Centers (SOCs).

There are, however, a few caveats to be noted: First, the proposed framework is analytical, not empirical, and thus needs to be validated in future with operational cybersecurity datasets or simulation-based experiments. Second, the Colonial Pipeline incident is used as an illustrative application and not as the basis for statistical inference, so findings are limited to applying the incident to the population in general. Third, it assumes that the attacker and defender are rational decision makers; however, in actual cyber operations, other factors such as organizational constraints, cognitive biases, political factors, and lack of intelligence can be at play. The framework should thus be tested in the future using agent-based simulations, cyber-game experiments repeated, or data sets from actual incidents to evaluate its predictive ability in various operational scenarios.

In conclusion, the proposed framework highlights the broader implications of AI-driven Cyber Threat Intelligence, extending beyond the technical realm of threat detection. It combines the generation of intelligence with Dynamic Bayesian decision-making, giving a theoretically based approach to the analysis of strategic cyber conflict under changing information conditions, and laying a groundwork for future analytical and empirical studies in cyber security.

CONCLUSION

As cyber threats grow more complex and the proliferation of Artificial Intelligence (AI) tools enters the landscape, cybersecurity no longer consists of just a technical field of study, but is a strategic challenge in decision-making. In today's cyber conflicts, information is incomplete, adversaries are adapting, and intelligence is evolving continuously, making it increasingly difficult to build up a model of uncertainty and dynamic strategic interactions. The research body has made substantial progress in the fields of AI-aided Cyber Threat Intelligence (CTI)

and game-theoretic Cybersecurity, but there has been little focus on how these fields can be integrated into a cohesive strategy for Cybersecurity decision making.

To fill that gap, this study proposed a Dynamic Bayesian Game-Theoretic Framework that combines the use of AI-assisted CTI and Bayesian decision-making under uncertainty. The proposed framework differs from traditional cybersecurity game models, which usually consider intelligence to be a static exogenous factor, by introducing AI-generated cyber intelligence as an endogenous strategic factor that continually evolves with the defender's belief and can affect the behavior of the defender and the attacker based on repeated interaction in the game. The framework includes the development of evolving intelligence, making it more realistic to reflect the current cyber operation where there is a continuous learning curve for both attackers and defenders.

The framework can be applied in practice to analyze the effects of the Colonial Pipeline ransomware attack, highlighting its value for understanding strategic decision-making in the event of a cyber incident affecting critical infrastructure. The case illustrates the advantages of using AI-powered CTI to mitigate information asymmetry, enhance situational awareness, and facilitate more informed defensive actions amidst uncertainty. The framework, while not an empirical predictive system, provides a structured way of assessing the interplay between intelligence generation, Bayesian learning and strategic adaptation in cybersecurity.

In three important ways, the study contributes to the literature. First, by bringing intelligence generation into the strategic decision-making process, it creates a seamless experience where AI-assisted Cyber Threat Intelligence is not just a separate component but a core part of the strategic framework. First, it eliminates the conceptual gap between AI-assisted Cyber Threat Intelligence and game-theoretic cybersecurity by integrating the intelligence generation into the strategic decision-making process. Second, it introduces Bayesian cybersecurity modelling and approach, which changes the paradigm of cybersecurity modelling from an assumption to a strategic resource. Third, it offers a foundation for future analysis to be used in cyber resilience research, ransomware response, critical infrastructure protection and decision-support using AI.

There are a number of caveats to note. The proposed framework has been presented in the context of a single case application and needs to be further tested via simulation experiments, operational cyber security data, or multiple cyber incident case studies. Apart from this, the model assumes that the actors behave rationally and does not explicitly take into account factors, such as organizational, behavioral, and geopolitical, that could affect cyber decision-making in reality.

Future models could be further strengthened if they could include these dimensions.

Future work should include the extension of the framework, with the incorporation of reinforcement learning, adversarial machine learning, multi-agent decision systems and empirical validation with real-world cyber threat intelligence datasets. This would make Dynamic Bayesian models more useful and add to the design of more adaptive and intelligence-based cybersecurity strategies that can address the more complex cyber threats.

REFERENCES

Alpcan, T., & Başar, T. (2010). An intrusion detection game with limited observations. In *Proceedings of the 12th International Symposium on Dynamic Games and Applications*. (Use only if cited in the text.)

Alpcan, T., & Başar, T. (2011). *Network Security: A Decision and Game-Theoretic Approach*. Cambridge University Press.

Balasubramanian, P., et al. (2025). Generative AI for cyber threat intelligence: Applications, challenges, and future directions. *Artificial Intelligence Review*. <https://doi.org/10.1007/s10462-025-11338-z>

Bratsas, C., Anastasiadis, E. K., Angelidis, A. K., Ioannidis, L., Kotsakis, R., & Ougiaroglou, S. (2024). Knowledge graphs and semantic web tools in cyber threat intelligence: A systematic literature review. *Journal of Cybersecurity and Privacy*, 4(3), 518–545. <https://doi.org/10.3390/jcp4030025>

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>

Cybersecurity and Infrastructure Security Agency. (2021). *DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks*. U.S. Department of Homeland Security. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>

Do, C. T., Tran, N. H., Hong, C. S., Kamhoua, C. A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N., & Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys*, 50(2), Article 30. <https://doi.org/10.1145/3057268>

European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

Federal Bureau of Investigation. (2021, May 10). *FBI statement on compromise of Colonial Pipeline networks*. <https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks>

Harsanyi, J. C. (1967). Games with incomplete information played by Bayesian players, Part I: The basic model. *Management Science*, 14(3), 159–182. <https://doi.org/10.1287/mnsc.14.3.159>

Harsanyi, J. C. (1968). Games with incomplete information played by Bayesian players, Part II: Bayesian equilibrium points. *Management Science*, 14(5), 320–334. <https://doi.org/10.1287/mnsc.14.5.320>

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. In *Proceedings of the 6th International Conference on Information Warfare and Security* (pp. 113–125).

Li, B., et al. (2025). CyberKG: Constructing a cybersecurity knowledge graph from cyber threat intelligence using domain-specific language models. *Future Internet*, 12(3), Article 100.

Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., & Hubaux, J.-P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys*, 45(3), Article 25. <https://doi.org/10.1145/2480741.2480742>

Mavroeidis, V., & Bromander, S. (2021). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *Future Internet*, 13(2), 42. <https://doi.org/10.3390/fi13020042>

MITRE Corporation. (2024). *MITRE ATT&CK® Framework*. <https://attack.mitre.org/>

Myerson, R. B. (1991). *Game Theory: Analysis of Conflict*. Harvard University Press.

Nash, J. (1951). Non-cooperative games. *Annals of Mathematics*, 54(2), 286–295. <https://doi.org/10.2307/1969529>

Nash, J. F. (1950). Equilibrium points in n -person games. *Proceedings of the National Academy of Sciences*, 36(1), 48–49. <https://doi.org/10.1073/pnas.36.1.48>

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. <https://doi.org/10.6028/NIST.AI.100-1>

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF 2.0)*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>

Osborne, M. J., & Rubinstein, A. (1994). *A Course in Game Theory*. MIT Press.

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, 25(14), 4272. <https://doi.org/10.3390/s25144272>

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies,

strategies, and collaborations in combating modern threats. *Sensors*, 25(14), 4272. <https://doi.org/10.3390/s25144272>

U.S. Department of Justice. (2021, June 7). *Department of Justice seizes \$2.3 million in cryptocurrency paid to the DarkSide ransomware group*. <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

U.S. Government Accountability Office. (2022). *Critical infrastructure protection: Actions needed to better secure pipelines against cybersecurity threats* (GAO-22-104625). <https://www.gao.gov/products/gao-22-104625>

Vassilev, A., Oprea, A., Fordyce, D., & Anderson, H. (2025). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2025). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-2e2025>

Von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton University Press.

Von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton University Press.