Article

A Game Theoretical Approach for Quantification of Strategic Behaviors in Digital Forensic Readiness

Mehrnoush Vaseghipanah , Sam Jabbehdari * , Hamidreza Navidi

Posted Date: 16 October 2025

doi: 10.20944/preprints202510.1285.v1

Keywords: digital forensic readiness; advanced persistent threats (APT); resource constraints; small and medium-sized enterprises (SMEs); MITRE ATT&CK; MITRE D3FEND; game theory; cybersecurity; security threats; artificial intelligence (AI); cybersecurity awareness

Article

A Game Theoretical Approach for Quantification of Strategic Behaviors in Digital Forensic Readiness

Mehrnoush Vaseghipanah [1], Sam Jabbehdari [1,*] and Hamidreza Navidi [2]

[1] Department of Computer, Tehran North Branch, Islamic Azad University, Tehran, Iran
[2] Department of Mathematics and Computer Sciences, Shahed University, Tehran, Iran
* Correspondence: sam.jabbehdari@iau.ac.ir

Abstract

Small and Medium-sized Enterprises (SMEs) face disproportionately high risks from Advanced Persistent Threats (APTs), which often evade traditional cybersecurity measures. While existing frameworks catalogue adversary tactics and defensive solutions, they offer limited quantitative guidance for optimal resource allocation under uncertainty—a challenge intensified by the proliferation of AI, which empowers both adaptive attacks and forensic complexity. To address this gap, we propose a novel game-theoretic model for enhancing Digital Forensic Readiness (DFR). Our methodology integrates the MITRE ATT&CK and D3FEND frameworks to systematically map APT behaviors to defensive countermeasures. We then define 32 custom DFR metrics, weighted via the Analytic Hierarchy Process (AHP), to compute quantitative utility functions for both adversaries and defenders. Equilibrium analysis reveals one Pure Nash Equilibrium (PNE) and five Mixed Nash Equilibria (MNE), indicating that allocating 90–95% of resources to proactive control modeling, while reserving a smaller portion for real-time detection, yields optimal strategic resilience. Simulations demonstrate that this strategy reduces attacker success rates by up to 30% in multi-vector APT scenarios. Furthermore, comparative analysis shows that SMEs with weak logging and limited forensic capabilities suffer 15–25% higher attack success rates; however, readiness improves markedly with enhanced data preservation and logging quality. Although the model's precision depends on AHP weighting assumptions, the proposed framework provides SMEs with actionable, equilibrium-informed strategies to significantly improve forensic preparedness and mitigate advanced cyber threats.

Keywords: digital forensic readiness; advanced persistent threats (APT); resource constraints; small and medium-sized enterprises (SMEs); MITRE ATT&CK; MITRE D3FEND; game theory; cybersecurity; security threats; artificial intelligence (AI); cybersecurity awareness

1. Introduction

Digital forensic readiness (DFR) enables organizations to proactively collect and preserve admissible digital evidence, reducing legal risks and supporting business continuity. It is particularly valuable for Small and Medium-sized Businesses and Enterprises (SMBs/SMEs)—encompassing both the commercial/business context (SMB) and the broader organizational/industrial context (SME)—which often face resource constraints in cybersecurity operations. A robust DFR strategy ensures that significant cyber incidents can be addressed efficiently, lawfully, and professionally, conserving investigative resources, reducing costs, protecting organizational reputation, and maintaining compliance with applicable regulations.

Despite heavy investment in Computer Security Incident Response Teams (CSIRTs), Digital Forensics and Incident Response (DFIR) units, and advanced monitoring technologies—such as EDR, XDR, NDR, SIEM, and IDPS—organizations still struggle to achieve effective incident detection and response. Such limitations become especially pronounced against Advanced Persistent Threats (APTs), which are sophisticated, well-funded actors conducting prolonged cyber campaigns APTs are stealthy,

 doi:10.20944/preprints202510.1285.v1

long term cyberattacks by unauthorized entities to remain undetected in networks [1–3]. Studies indicate that the average dwell time before breach detection exceeds 190 days, granting adversaries ample time for network infiltration and data exfiltration [4]. Moreover, about 60% of small enterprises cease operations within six months of a major incident [5]. For example, Baker [6] notes that in the SolarWinds incident, threats persisted within networks for prolonged periods without detection.

The rapid proliferation of artificial intelligence (AI) has further complicated this landscape. AI-driven tools empower attackers with advanced automation, adaptive tactics, and the ability to launch more sophisticated and targeted attacks, thereby increasing the potency of APTs. Conversely, while AI offers defenders enhanced capabilities for faster and more accurate detection, it also introduces unprecedented forensic challenges. These include the complexity of analyzing AI-generated attacks, the potential for AI-based evidence manipulation, and the need for new techniques to handle AI-related incidents. For SMBs, these challenges are particularly acute due to resource constraints. These technical challenges are compounded by the broader organizational struggle to effectively govern AI systems and mitigate associated risks, a problem highlighted in recent literature [7].

Organizations often perceive this issue as primarily technical in nature. However, this challenge fundamentally encompasses the interplay of technology, human expertise, and processes. Without skilled personnel and planning, even the most advanced technology stack may fail against determined assailants. We use the term 'non-forensicability' to refer to situations where inadequate DFR hinders effective cyber security incident investigations, often due to poor data retention, ineffective log management, or compromised digital evidence integrity. Wrightson [8] emphasizes that understanding an attacker's motivations and capabilities, as well as knowing their past actions, helps investigators categorize and respond to diverse cyber threats.

Digital forensic investigators must know both defense and offense strategies, preempt emerging attack techniques, and collaborate closely with defense teams. Årnes [9] characterizes digital forensics, as a sub-discipline of forensic science, as encompassing scientifically validated methods for the management of digital evidence. These methods are essential for reconstructing criminal incidents or anticipating unauthorized activities.

To address the need for a formal strategic framework for DFR, we propose a game-theoretic approach to model the strategic interactions between cyber attackers and defenders. This approach helps organizations anticipate threats, optimize defense strategies, and make more informed decisions. We focus on the strategic behavior in digital forensics, drawing from Sun Tzu's wisdom in 'The Art of War,' which emphasizes the importance of understanding both one's own abilities and the opponent's strengths and strategies. As Tzu [10] states, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. You will succumb in every battle if you know neither the enemy nor yourself." This highlights the importance of knowing the adversary's motivations, methods, and goals, as well as the capabilities and limitations of one's own tools and techniques.

Inspired by Sun Tzu's philosophy, our game-theoretic model operationalizes this wisdom by quantifying how knowledge asymmetries between attacker and defender impact forensic readiness. We formalize three strategic states: comprehensive knowledge (targeted defense), partial knowledge (vulnerable defense), and ignorance (minimal resilience). This approach is especially important in the AI era, where modeling emerging AI-powered attack surfaces and their forensic implications becomes essential for building resilient systems.

Game theory provides a mathematical foundation for analyzing strategic interactions among rational decision-makers [11]. Its application in cybersecurity is growing, as it offers a structured approach to:

- **Model Strategic Decisions**: Capture the objectives and constraints of both attackers and defenders [12].
- **Conduct Risk Analysis**: Elucidate payoffs and tactics to identify critical vulnerabilities and optimal defensive strategies [13].

 doi:10.20944/preprints202510.1285.v1

- **Enable Adaptive Defense**: Capture the dynamic nature of cyber threats, including those augmented by AI, to inform adaptive countermeasures [14].
- **Optimize Resource Allocation**: Evaluate strategy effectiveness to guide efficient investment of limited defensive resources [15].

To operationalize this game-theoretic approach, our methodology is grounded in established cybersecurity standards and formal decision-making processes. We build upon best practices from the National Institute of Standards and Technology (NIST) for metric development and forensic readiness [16]. Specifically, we integrate the MITRE ATT&CK framework to systematically model adversary behaviors and the complementary MITRE D3FEND framework to map defensive countermeasures. This integration provides a standardized taxonomy that bridges attacker tactics with defender responses. Based on these frameworks, we define 32 custom DFR metrics, weighted using the Analytic Hierarchy Process (AHP), to compute quantifiable utility functions for both attackers and defenders. This addresses a critical gap in the field: the absence of quantifiable payoffs in strategic DFR planning. Furthermore, we present an end-to-end algorithmic suite for scoring, classification, and gap analysis, moving beyond fragmented assessments towards a holistic readiness model.

This paper makes the following key contributions:

- A novel game-theoretic model for DFR that quantifies strategic attacker-defender interactions.
- The integration of MITRE ATT&CK and D3FEND with AHP-weighted metrics to ground utilities in real-world tactics and techniques.
- An equilibrium analysis that yields actionable resource allocation guidance for SMBs/SMEs.
- An evaluation demonstrating the framework's efficacy in reducing attacker success rates, even in complex, multi-vector APT scenarios influenced by modern AI-powered tools.

The remainder of this paper is structured as follows: Section 2 reviews the related works in digital forensics investigation and readiness. Section 3 describes our game-theoretic approach and algorithms for DFR. Section 4 presents our experimental analysis and results. Section 5 concludes with our findings and future work.

2. Related Works

Enhancing cybersecurity and digital forensics has spurred a plethora of studies. These foundational works span technical defenses, strategic modeling, and simulation of cyber interactions. While appreciating their contributions, we identify areas for further exploration.

2.1. Game Theory in Digital Forensics

Alpcan et al. [17] provided a foundational contribution to the field of network security by presenting theoretical approaches for decision-making in security from a game-theoretic perspective. Their work serves as a valuable reference not only for researchers and graduate students but also for practitioners such as system administrators and security officers seeking to apply quantitative models grounded in control, optimization, and decision theory. Casey [18] established the conceptual foundation for incorporating game theory into digital forensics, contextualizing how strategic analysis can enhance forensic practices.

Manshaei et al. [19] offered a comprehensive overview of game-theoretic methods in network security and privacy, highlighting their capability to model strategic interactions in complex adversarial environments. Their study provided in-depth insights into how game theory can strengthen computer and communication network security across multiple layers, including physical and MAC layers, self-organizing networks, intrusion detection systems, anonymity and privacy mechanisms, network security economics, and cryptography. The authors summarized key concepts such as equilibrium analysis and mechanism design, emphasizing the significance of addressing information limitations and learning factors in developing effective security solutions.

Several subsequent studies have built on this foundation to explore game-theoretic applications in digital forensics. Nisioti et al. [20] presented a Bayesian game model for analyzing interactions

 doi:10.20944/preprints202510.1285.v1

between a forensic investigator and a strategic attacker on a multi-host forensic investigation graph. Hasanabadi et al. [21] developed a model representing attacker–investigator dynamics involving rootkits and anti-rootkits, defining each player's actions and profiling their characteristics. Extending these ideas, Karabiyik et al. [22] proposed a game-theoretic approach to optimize tool selection in digital forensics, particularly focusing on file carving tools and the strategic adaptation of selection decisions during investigations. Hasanabadi et al. [23] later introduced a memory-based mechanism to expand action spaces within forensic game models, reducing convergence iterations when new anti-forensic or counter-anti-forensic tools emerge. Caporusso et al. [24] further analyzed post-attack decision dynamics in human-controlled ransomware scenarios, modeling negotiation strategies and emphasizing the role of information availability, user education, and human factors in developing resilient defensive responses.

2.2. Digital Forensics Readiness and Techniques

Kebande et al. [25] introduced a technique for implementing DFR in cloud computing environments through a modified obfuscated Non-Malicious Botnet (NMB). Operating as a distributed forensic Agent-Based Solution (ABS), this method enables forensic logging for readiness purposes across cloud infrastructures. In a related effort, Kebande et al. [26] proposed the construction of a Digital Forensic Readiness Intelligence Repository (DFRIR) founded on knowledge-sharing principles. The repository cross-references potential evidence sources, aims to reduce the time required for forensic investigations, and supports sharing across multiple jurisdictions.

Englbrecht et al. [27] developed a DFR-specific Capability Maturity Model (CMM) to guide organizations in implementing readiness measures. The framework draws on COBIT 5 IT-Governance principles and incorporates the core characteristics necessary for effective DFR implementation. Reddy et al. [28] built a Digital Forensic Readiness Management System (DFRMS) tailored for large organizations. Based on requirements identified through a comprehensive literature review, the DFRMS architecture comprises five modules: event analysis, DFR information management, costing, access control, and user interface. A proof-of-concept prototype demonstrated the system's practical feasibility and its potential to improve readiness in enterprise contexts.

Grobler et al. [29] positioned DFR as a means to strengthen organizational security strategies by preparing for incidents while minimizing disruptions to business processes. Their guidelines emphasize ensuring legal admissibility of evidence, detecting resource misuse, and demonstrating due diligence in protecting valuable company assets. The authors contend that revisions to current information systems architectures, strategies, and best practices are needed to enable successful prosecutions, pointing to deficiencies in admissible evidence and procedural rigor. Lakhdhar et al. [30] proposed a game-theoretic model for forensic-ready systems utilizing cognitive security concepts; however, this work lacks practical tools applicable to SMBs/SMEs.

Elyas et al. [31] designed and validated a DFR framework through expert focus groups. The framework assists organizations in assessing their forensic strategies by identifying critical factors in capacity development. It categorizes governance, top management support, and culture as organizational dimensions, while technology and architecture are grouped under forensic infrastructure. Baiquni and Amiruddin [32] applied the Digital Forensic Readiness Index (DiFRI) to quantitatively evaluate a cyber organization's operational readiness, offering tailored improvement recommendations. Although informative, this methodology does not address strategic adversary behavior or optimal resource allocation—gaps targeted by our proposed game-theoretic approach.

Complementing DFR frameworks with an SME-focused perspective, Rawindaran et al. [33] introduce an enhanced ROHAN model integrated with the Cyber Guardian Framework (CGF) to improve cybersecurity resilience in resource-constrained organizations. Their mixed-methods study emphasizes role-specific awareness, continuous improvement, and the use of AI-enabled decision support—principles aligned with readiness thinking. However, while ROHAN+CGF advance organizational practice, they do not explicitly model adversarial strategy or attacker–defender interdependence;

 doi:10.20944/preprints202510.1285.v1

our game-theoretic formulation targets precisely this gap by coupling readiness with strategic behavior and optimal resource allocation.

Trenwith et al. [34] advocated centralized logging as a cornerstone of effective DFR, enabling rapid acquisition of evidential data and accelerated investigative analysis. While centralized log management streamlines evidence collection, it does not account for the diverse evidence types necessary in investigations, particularly within cloud environments. Cloud systems present additional challenges due to the dynamic and distributed nature of data storage and processing, which demand solutions beyond efficient logging.

In the context of microservice architectures, Monteiro et al. [35] proposed "Adaptive Observability," a game theory-driven method designed to address evidence challenges in ephemeral environments where traditional observability mechanisms fail after container termination. By dynamically adjusting observability based on user–service interactions, the approach enhances evidence retention while optimizing resource consumption. Comparative evaluations show performance improvements ranging from 3.1 % to 42.50 % over conventional techniques. The authors suggest future work should incorporate varying attacker risk preferences and extend into industrial case studies, with additional metrics covering cost-effectiveness and scalability.

2.3. Advancement in Cybersecurity Modeling

Xiong et al. [36] developed a threat modeling language for enterprise security based on the MITRE Enterprise ATT&CK Matrix and implemented using the Meta Attack Language framework. This language enables the simulation of cyberattacks on modeled system instances to analyze security configurations and assess potential architectural modifications aimed at improving system resilience.

Wang et al. [37] proposed a sequential Defend-Attack framework that integrates adversarial risk analysis. Their approach introduces a new class of influence diagram algorithms, termed hybrid Bayesian network inference, to identify optimal defensive strategies under adversarial conditions. This model enhances understanding of the interdependent decision processes between attackers and defenders in dynamic threat environments.

Usman et al. [38] presented a hybrid methodology for IP reputation prediction and zero-day attack categorization that fuses Dynamic Malware Analysis, Cyber Threat Intelligence, Machine Learning, and Data Forensics. This integrated system simultaneously evaluates severity, risk score, confidence, and threat lifespan using machine learning techniques, illustrating how data-driven analytics can support forensic and security objectives. The study also highlights persistent data forensic challenges when automating classification and reputation modeling for emerging cyber threats.

2.4. Innovative Tools and Methodologies

Li et al. [39] introduced *LEChain*, a blockchain-based lawful evidence management scheme for digital forensics designed to address security and privacy concerns often overlooked in cloud computing and blockchain-based evidence management. LEChain implements fine-grained access control through ciphertext-policy attribute-based encryption and employs brief randomizable signatures to protect witness privacy during evidence collection.

Soltani and Seno [40] presented a Software Signature Detection Engine (SSDE) for digital forensic triage. The SSDE architecture comprises two subsystems: signature construction and signature detection. Signatures are generated using a differential analysis model that compares file system states before and after execution of specific software. Their study evaluates multiple design parameters, resulting in the creation and assessment of 576 distinct SSDE models.

At the storage–firmware boundary, Rother and Chen [41] present *ACRecovery*, a flash-translation-layer (FTL) forensics mechanism that can roll back OS access-control metadata after an OS-level compromise by exploiting out-of-place updates in raw flash. Their prototype on EXT2/EXT3 and OpenNFM demonstrates efficient recovery with minimal performance impact, highlighting a promising post-compromise remediation path. While orthogonal to our strategic readiness modeling, such FTL-

 doi:10.20944/preprints202510.1285.v1

aware techniques complement DFR by preserving evidential integrity and enabling rapid restoration when preventive controls are bypassed.

Nikkle [42] described the Registration Data Access Protocol (RDAP) as a secure, standardized, and internationalized alternative to the legacy WHOIS system. While WHOIS and RDAP are expected to coexist for some time, RDAP offers enhanced security, automation capabilities, tool integration, and authoritative data sourcing—features that strengthen its utility in digital forensic investigations. Furthermore, Nikkle [43] introduced the concept of *Fintech Forensics* as a new sub-discipline, noting how the rise of digital transformation and financial technology has created novel avenues for criminal activity, necessitating dedicated forensic methodologies for financial transactions.

2.5. Digital Forensics in Emerging Domains

Seo et al. [44] proposed a Metaverse forensic framework structured around four phases derived from NIST's digital forensic guidelines: data collection, examination and retrieval of evidence, analysis, and reporting. The study also outlines three procedures for data collection and examination distributed across user, service, and Metaverse platform domains, providing a systematic approach for investigating offenses occurring in virtual environments.

Malhotra [45] explored the intersection of digital forensics and artificial intelligence (AI), presenting current approaches and emerging trends. The author emphasized that in today's increasingly digital society, the rise in cybercrimes and financial frauds has made digital forensics indispensable. Integrating AI techniques into forensic analysis offers promising opportunities to address these challenges effectively. Malhotra further argued that AI-driven digital forensics could transform investigative efficiency, catalyzing the so-called Fourth Industrial Revolution. Consequently, continued investment in AI-enabled forensic technologies, specialized training, and advanced analytical tools is critical for ensuring preparedness against evolving cyber threats.

Tok and Chattopadhyay [46] examined cybersecurity challenges within Smart City Infrastructures (SCI), proposing a unified definition and applying the STRIDE threat modeling methodology to identify potential offenses and evidence sources. Their study provides valuable guidance for investigators by mapping technical and legal aspects of digital forensics in SCI environments. However, the authors note that the applicability of their framework may depend on contextual variations in regulatory standards and implementation practices across jurisdictions.

2.6. Advanced Persistent Threats and Cybercrime

Han et al. [47] examined defensive strategies against long-term and stealthy cyberattacks, such as Advanced Persistent Threats (APTs). Their work underscores the necessity of strategic and proactive measures to counter increasingly sophisticated adversaries capable of prolonged network infiltration.

Chandra and Snowe [48] defined cybercrime as criminal activity involving computer technology and proposed a taxonomy built upon four foundational principles: mutual exclusivity, structural clarity, exhaustiveness, and well-defined categorization. This taxonomy facilitates the classification and differentiation of various cybercrime types and could be extended to organizational applications, metrics development, integration with traditional crime taxonomies, and automated classification for improved efficiency.

Collectively, these contributions highlight the potential of combining game theory with advanced technologies—such as artificial intelligence and blockchain—to enhance the effectiveness of digital forensic investigations. Casey et al. [49] introduced the Cyber-investigation Analysis Standard Expression (CASE), a community-driven specification language designed to improve interoperability and coordination among investigative tools. By building upon the Unified Cyber Ontology (UCO), CASE offers a standardized structure for representing and exchanging cyber-investigation data across multiple organizations and jurisdictions. Its versatility allows application in criminal, corporate, and intelligence contexts, supporting comprehensive analysis. Through illustrative examples and a proof-of-concept API, Casey et al. demonstrated how CASE enables structured data capture, facilitates

 doi:10.20944/preprints202510.1285.v1

sharing and collaboration, and incorporates data marking for controlled dissemination within the cyber-investigation community.

Despite notable progress in cybersecurity and digital forensics—particularly via the integration of game theory, enhanced readiness techniques, and diverse modeling tools—several critical challenges remain. Current approaches often struggle to represent the dynamic and asymmetric interactions between attackers and defenders in APT scenarios. Moreover, game-theoretic models frequently overlook nuanced decision-making processes inherent to forensic investigations and fail to fully account for the rapidly evolving tactics of modern cyber adversaries. Additionally, many DFR frameworks emphasize technical countermeasures while insufficiently addressing strategic adversary dynamics, leaving organizations vulnerable and less responsive to emerging threats.

3. Materials and Methods

In this section, the problem statement is provided in Subsection 3.1. The methodology of the research is stated in Subsection 3.2. The fundamental concepts of game theory are presented in Subsection 3.3. The proposed approach is detailed in Subsection 3.4, followed by the utility function discussion in Subsection 3.5. The identification of improvement areas and prioritization of DFR are addressed in Subsections 3.6 and 3.7, respectively. The reevaluation of DFR is covered in Section 3.8.

3.1. Problem Statement

Let A represent the set of attackers and D represent the set of defenders in a cyber environment. The objective of this research is to model the strategic interactions between A and D during the DFR phase using game theory.

Let us define the following variables:

- S_A: Strategies available to attackers, corresponding to MITRE ATT&CK tactics (e.g., Reconnaissance, Resource Development, Initial Access, Execution, Persistence, etc.).
- S_D: Strategies available to defenders, corresponding to MITRE D3FEND countermeasures (e.g., Model, Detect, Harden, Isolate, Deceive, etc.)
- P: Parameters influencing game models, such as attack severity, defense effectiveness, and forensic capability.
- $U_A(s_A, s_D)$: Utility function for attackers, representing the payoff based on their strategy s_A and the defenders' strategy s_D.
- $U_D(s_A, s_D)$: Utility function for defenders, representing the payoff based on their strategy s_D and the attackers' strategy s_A.

The research aims to solve the following problems:

- **Model Construction**: Construct game models $G(A, D, S_A, S_D, P)$ to represent the interactions between A and D.
- **Equilibrium Analysis**: Identify Nash equilibria (s_A^*, s_D^*) such that:

$$U_A(s_A^*, s_D^*) \geq U_A(s_A, s_D^*) \quad \forall s_A \in S_A$$
$$U_D(s_A^*, s_D^*) \geq U_D(s_A^*, s_D) \quad \forall s_D \in S_D$$

The goal is to derive optimal strategies (s_A^*, s_D^*) that enhance DFR, thereby informing the development of effective cybersecurity policies and strategies. This research contributes to the theoretical understanding of strategic interactions in cybersecurity, providing a foundation for future empirical studies and practical applications.

3.2. Methodology

This subsection outlines the research methodology, which is structured around the following components:

 doi:10.20944/preprints202510.1285.v1

3.2.1. Research Design

- **Theoretical Framework**: The study employs game theory to analyze strategic interactions between attackers and defenders in the context of DFR.
- **Model Representation**: Game theory models are used to represent the decision-making process of both attackers and defenders, considering their incentives, strategies, and potential outcomes.

3.2.2. Materials

The primary materials used in the research include:

- **Game Theory**: The research uses game theory literature to build theoretical foundations and employ advanced modeling techniques for analyzing the strategic interactions between attackers and defenders.
- **DFR Frameworks**: The study uses established DFR frameworks to understand the requirements and strategies involved so our models reflect real world forensic readiness scenarios.
- **Computational Tools and Software**: Advanced computational tools and software are used to simulate game scenarios and analyze the strategic behavior of both attackers and defenders. These tools allow us to model complex interactions and generate insights from the simulations.

3.2.3. Procedure

- **Development of Game Models**: Construct game models to represent the interactions between attackers and defenders in DFR scenarios.
- **Identification of Strategies**: Define strategies available to attackers and defenders, such as investing in security measures, launching attacks, or conducting forensic investigations.
- **Parameterization**: Assign values to parameters within the game models, representing factors like attack severity, defense effectiveness, and forensic capability.
- **Simulation and Analysis**: Simulate scenarios using game-theoretic algorithms to evaluate model performance and outcomes.
- **Sensitivity Analysis**: Conduct sensitivity analysis to assess the impact of varying parameters on strategic outcomes and forensic readiness scores.

3.2.4. Data Analysis

- **Quantification of Strategic Behaviors**: Quantify the strategic behaviors of attackers and defenders based on game-theoretic metrics such as equilibrium outcomes, payoffs, and dominance strategies.
- **Interpretation**: Interpret the results of the analysis to identify optimal strategies for improving DFR, including investment priorities, resource allocation, and policy adjustments.

3.2.5. Validation

- **Validation of Model Assumptions**: Validate game models against real-world scenarios and empirical data where possible, ensuring that the theoretical framework accurately captures the dynamics of DFR.
- **Sensitivity Testing**: Perform sensitivity testing to assess the robustness of the findings against variations in the assumptions and parameters of the model.

3.2.6. Reporting

- **Documentation**: Document the methodology, assumptions, and results of the study in a comprehensive research report or academic paper.
- **Discussion**: Discuss the implications of the findings for improving DFR, addressing limitations, and suggesting avenues for future research.

This study aims to provide valuable information on the strategic behaviors of attackers and defenders in DFR scenarios, forming the development of more effective cybersecurity strategies and policies.

 doi:10.20944/preprints202510.1285.v1

3.3. Game Theory Background

Game theory provides a framework for analyzing strategic decision-making among agents, or players, whose choices influence one another's outcomes.

3.3.1. Players and Actions

We focus on games with a finite number of players, denoted by $N = \{1, 2, ..., n\}$. Each player i has a set of available actions represented by A_i. The combination of all players' actions, called the action profile, is calculated using the Cartesian product:

$$A = A_1 \times A_2 \times \cdots \times A_n$$

3.3.2. Payoff Functions and Utility

Each player has a payoff function, denoted by $u_i : A \to \mathbb{R}$. This function maps an action profile $a = (a_1, a_2, ..., a_n)$ to a real number representing their utility or satisfaction with the outcome.

The payoff function captures the player's preferences, considering how their benefits depend on the actions chosen by all players. Digital forensics plays a crucial role in incident response, relying heavily on preparedness during the readiness phase. This section explores how game theory can be utilized to enhance decision-making in this critical stage.

3.3.3. Scenario Analysis

Consider a company (Defender) that anticipates potential data breaches and contemplates investing in additional forensic tools (FT) to improve their readiness. However, the optimal level of investment (High Investment: HI, Low Investment: LI) remains unclear. Simultaneously, an Attacker is contemplating the type of attack to launch: a sophisticated attack (SA) or a simpler attack (SI).

3.3.4. Formalizing the Game

This scenario can be modeled as a two-player, non-cooperative game with the following elements:

- **Players**: Defender (D), Attacker (A)
- **Actions**:
  - Defender: $D \in \{\text{HI FT}, \text{LI FT}\}$ (Set of defender's investment choices)
  - Attacker: $A \in \{\text{SA}, \text{SI}\}$ (Set of attacker's attack choices)
- **Payoff Functions**:
  - Defender's Payoff Function: $u_D(D, A)$ (Maps a combination of defender's investment (D) and attacker's attack (A) to a real number representing the defender's utility)
  - Attacker's Payoff Function: $u_A(D, A)$ (Maps a combination of defender's investment (D) and attacker's attack (A) to a real number representing the attacker's utility)

The interaction can be represented by the following payoff matrix:

Table 1. Payoff Matrix for Defender-Attacker Game.

	Attack (SA)	**Attack (SI)**
Defender (HI FT)	$(u_D(\text{HI FT}, \text{SA}), u_A(\text{HI FT}, \text{SA}))$	$(u_D(\text{HI FT}, \text{SI}), u_A(\text{HI FT}, \text{SI}))$
Defender (LI FT)	$(u_D(\text{LI FT}, \text{SA}), u_A(\text{LI FT}, \text{SA}))$	$(u_D(\text{LI FT}, \text{SI}), u_A(\text{LI FT}, \text{SI}))$

3.3.5. Payoff Analysis

Details of the payoff matrix are as follows:

- **Defender's Payoffs**:
  - **HI FT**: High investment in forensic tools leads to high readiness for a sophisticated attack (SA), resulting in low losses (high utility) for the defender. However, if the attacker chooses

 doi:10.20944/preprints202510.1285.v1

a simpler attack (SI), the high investment might be unnecessary, leading to very low losses (moderate utility) but potentially wasted resources.
  - **LI FT**: Low investment translates to lower readiness, making the defender more vulnerable to a sophisticated attack (SA), resulting in high losses (low utility). While sufficient for a simpler attack (SI), it might not provide a complete picture for forensic analysis, leading to moderate losses (moderate utility).
- **Attacker's Payoffs**:
  - **SA**: A sophisticated attack offers the potential for higher gains (data exfiltration) but requires more effort and resources to bypass advanced forensic tools (HI FT) implemented by the defender. If the defender has low investment (LI FT), the attack is easier to conduct, resulting in higher gains (higher utility).
  - **SI**: This requires less effort but might yield lower gains (lower utility). If the defender has high investment (HI FT), the attacker might face challenges in extracting data, resulting in very low gains (low utility).

This scenario represents a non-cooperative game where both players make independent decisions to maximize their own utility. A potential Nash Equilibrium exists where the defender chooses High Investment (HI FT) and the attacker chooses Simpler Attack (SI). The defender prioritizes high readiness, while the attacker avoids the risk of encountering advanced forensic tools.

This simple game shows the importance of considering attacker behavior in the readiness phase. By understanding attacker strategies through game theory, defenders can make informed decisions about where to allocate forensic tools and training.

3.3.6. Advanced Persistent Threats (APTs) and Equilibrium Concepts

APTs present a significant challenge due to their sophisticated, multi-stage attack lifecycle. Analyzing these dynamics requires equilibrium concepts beyond Pure Nash Equilibria (PNE). A Mixed Nash Equilibrium (MNE) is often more representative, as it models the strategic uncertainty where players randomize their actions. For instance, a defender, uncertain of the APT's exact target, might probabilistically allocate security resources across critical servers. Concurrently, the APT might randomize its attack vectors to avoid predictable patterns. This MNE state introduces optimal unpredictability, preventing either party from gaining an advantage by deviating unilaterally.

3.4. Proposed Approach

Inspired by Sun Tzu's strategic principles, our approach models digital forensics as a normal-form game between two primary entities: attacker and defender. This game captures their strategy sets and resulting payoffs as follows:

- **Players**:
  - Attacker: 14 strategies ($s_1, s_2, \ldots, s_{14}$)
  - Defender: 6 strategies ($t_1, t_2, \ldots, t_6$)
- **Payoff Matrices**: Shown in Table 2 for the attacker and Table 3 for the defender, each matrix displays payoffs for every strategy combination.
- **Rationality**: Both players are presumed rational, seeking to maximize their individual payoffs given knowledge of the opponent's strategy. The game is simultaneous and non-zero-sum.

Attacker strategies include actions such as reconnaissance, execution, privilege escalation, and others. Defender strategies encompass modeling, detecting, deceiving, and additional controls. Modeling these interactions provides insight into the dynamic strategic landscape of digital forensics. As visualized in Figure 1, analysis of the payoff matrices reveals both outcomes and equilibrium points, highlighting the evolving nature of cyber threats. Darker matrix shades indicate higher attacker payoffs.

 doi:10.20944/preprints202510.1285.v1

Table 2. Attacker's Payoff Matrix $A(s,t)$.

	t1	t2	t3	t4	t5	t6
s1	5	6	7	8	9	10
s2	0	0	1	2	3	4
s3	14	13	12	11	0	0
s4	16	17	18	18	0	0
s5	19	20	20	18	0	0
s6	23	22	21	7	6	5
s7	24	25	26	24	25	26
s8	32	28	29	30	33	32
s9	33	34	35	30	33	32
s10	32	35	36	6	7	5
s11	36	37	38	6	35	30
s12	37	38	39	39	0	0
s13	38	39	40	0	0	0
s14	39	40	41	0	0	0

Table 3. Defender's Payoff Matrix $D(s,t)$.

	t1	t2	t3	t4	t5	t6
s1	5	7	1	1	7	5
s2	6	8	10	2	6	6
s3	7	9	11	5	8	11
s4	8	10	25	25	9	12
s5	9	11	24	8	10	13
s6	10	12	24	8	11	10
s7	11	21	20	10	12	7
s8	18	14	25	9	5	25
s9	13	15	23	12	4	8
s10	14	16	22	11	14	9
s11	15	17	20	12	13	14
s12	16	18	21	13	15	25
s13	17	20	20	10	16	17
s14	12	19	29	16	17	16

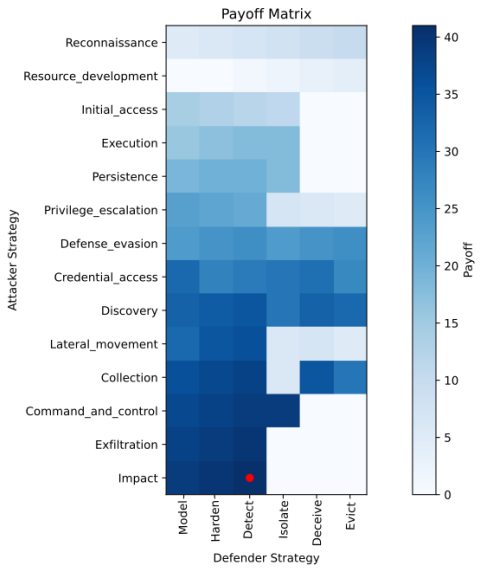


Figure 1. Visualization of payoff matrices depicting strategic interactions between attacker and defender. Darker shades indicate higher attacker payoffs.

 doi:10.20944/preprints202510.1285.v1

3.4.1. PNE Analysis

The PNE was determined using support enumeration [50], systematically exploring all possible strategy profiles. Starting from the smallest supports, we iteratively increased complexity and verified for PNE by ensuring each strategy profile was a mutual best response.

For example, for strategy s_{14}^* ('Impact') to form a Nash Equilibrium with the defender's strategy t_3^* ('Detect'), the following must hold:

$$A(s_{14}, t_3^*) \geq A(s_k, t_3^*) \quad \forall k \in \{1, 2, \ldots, 14\},\ k \neq 14 \tag{1}$$

This means 'Impact' gives the attacker at least as much payoff as any alternative when the defender uses 'Detect'. The reciprocal check for the defender is:

$$D(s_{14}^*, t_3) \geq D(s_{14}^*, t_l) \quad \forall l \in \{1, 2, 4, 5, 6\} \tag{2}$$

confirming that 'Detect' is optimal for the defender against 'Impact'. This NE is highlighted in Figure 1.

3.4.2. MNE Analysis

To capture the adaptive nature of cyber threats, we analyze MNE, where players randomize over multiple strategies. The triangular membership function in Algorithm 1, defined by parameters (a, b, c), is used for fuzzy payoff assessment:

$$\mu(x) = \begin{cases} \max\left(0, \min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}, 1\right)\right), & \text{if } a \leq x \leq c \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

This enables categorization of payoffs (e.g., "Low," "Medium," "High"), reflecting the fuzziness of real security outcomes. Tables 2 and 3 present the resulting values.

Algorithm 1 Attacker–Defender Payoff Matrix Calculation

Input: AttackTactics, DefenseTactics, FuzzySets, FuzzyRules
Output: FuzzyPayoffMatrix

```
Initialize FuzzyPayoffMatrix as empty
for each attacker tactic t do
    for each defense tactic d do
        FuzzyPayoffMatrix[(t, d)] ← (None, None)
for each rule r in FuzzyRules do
    for each cell (t, d) do
        if rule matches t and d then
            Compute and aggregate membership degree using triangular function
            Update FuzzyPayoffMatrix[(t, d)]
Defuzzify payoff values using the center-of-gravity method return FuzzyPayoffMatrix
```

3.4.3. Payoff Matrix Calculation Algorithm

Fuzzy payoff matrices are computed via Algorithm 1, which uses triangular membership definitions and fuzzy rule evaluation.

3.4.4. Payoff Matrices

The final payoff matrices for attacker and defender strategies are shown in Tables 2 and 3.

3.4.5. Mixed Nash Equilibrium Computation

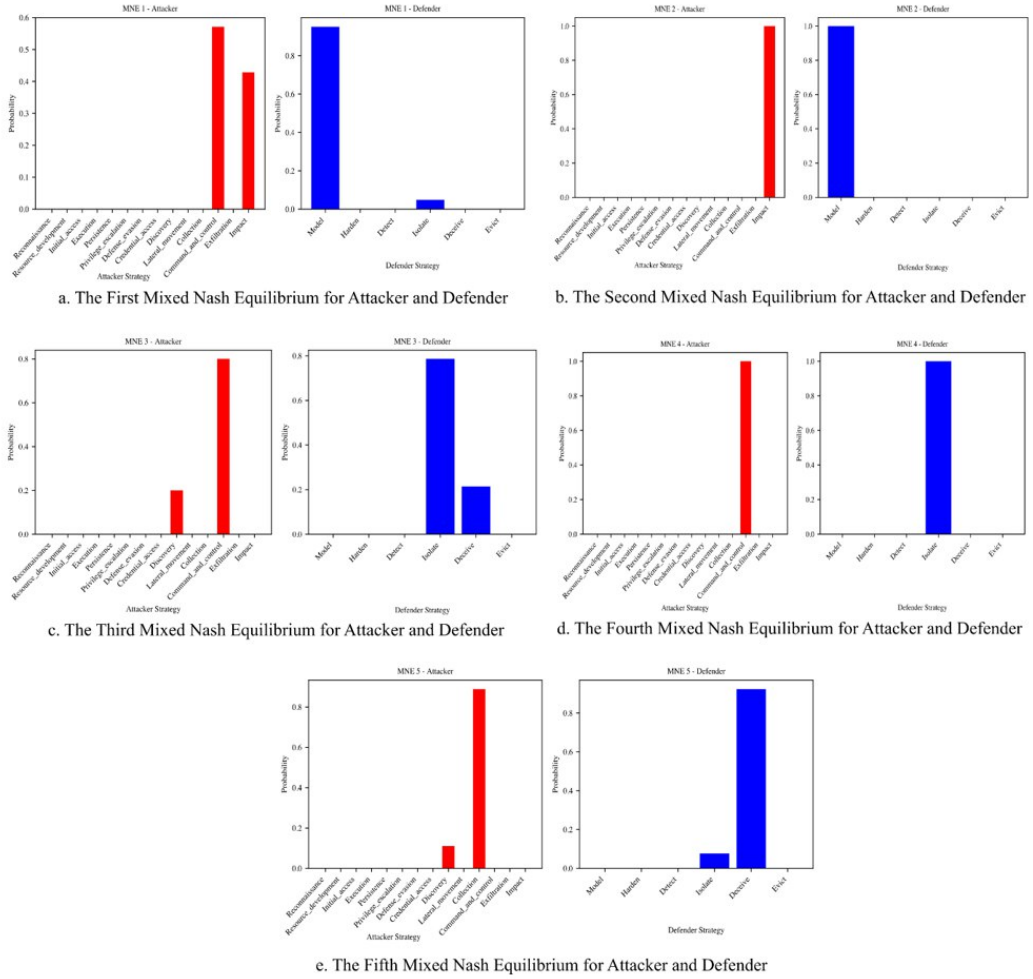
MNEs are computed through enumeration of pure strategy vertices, followed by construction of best-response polytopes for mixed strategies, as described in [50]. For payoff matrices A and D, an MNE consists of mixed strategies (x^*, y^*) fulfilling:

 doi:10.20944/preprints202510.1285.v1

$$\sum_{j=1}^{6}\sum_{i=1}^{14} a_{ij}x_i^*y_j^* \geq \sum_{j=1}^{6}\sum_{i=1}^{14} a_{ij}x_iy_j^* \quad \forall x \in \Delta_{14} \tag{4}$$

$$\sum_{i=1}^{14}\sum_{j=1}^{6} d_{ij}x_i^*y_j^* \geq \sum_{i=1}^{14}\sum_{j=1}^{6} d_{ij}x_i^*y_j \quad \forall y \in \Delta_{6} \tag{5}$$

Nashpy [51] is used for vertex enumeration. Analysis yielded five MNEs, each illustrating different patterns of mixed strategic play (see Figure 2).



a. The First Mixed Nash Equilibrium for Attacker and Defender

b. The Second Mixed Nash Equilibrium for Attacker and Defender

c. The Third Mixed Nash Equilibrium for Attacker and Defender

d. The Fourth Mixed Nash Equilibrium for Attacker and Defender

e. The Fifth Mixed Nash Equilibrium for Attacker and Defender

Figure 2. Probability distributions over attack tactics (red) and defensive controls (blue) in the five identified Mixed Nash Equilibria (MNE1–MNE5).

MNE Analysis Results

- **First MNE:** The attacker prefers 'Command_and_Control' (57%), while the defender favors 'Model' (95%) with some likelihood for 'Detect'.
- **Deterministic Scenarios:** Certain equilibria show exclusive preference (e.g., attacker fully on 'Exfiltration', defender on 'Model' or 'Detect').
- **Variable Strategies:** Some MNEs distribute probabilities across two or more strategies, reflecting tactical unpredictability.

3.4.6. Convergence Analysis

Convergence points (Figure 3) represent stable game states where each player's optimal mixed strategy is fixed, given the opponent's choices. Let α^* and β^* denote the optimal mixed strategies for attacker and defender, respectively:

 doi:10.20944/preprints202510.1285.v1

$$A(S_k, \alpha^*, \beta^*) \succeq A(s, \alpha^*, \beta^*) \quad \forall s \in S \tag{6}$$

$$D(t_l, \alpha^*, \beta^*) \succeq D(t, \alpha^*, \beta^*) \quad \forall t \in T \tag{7}$$

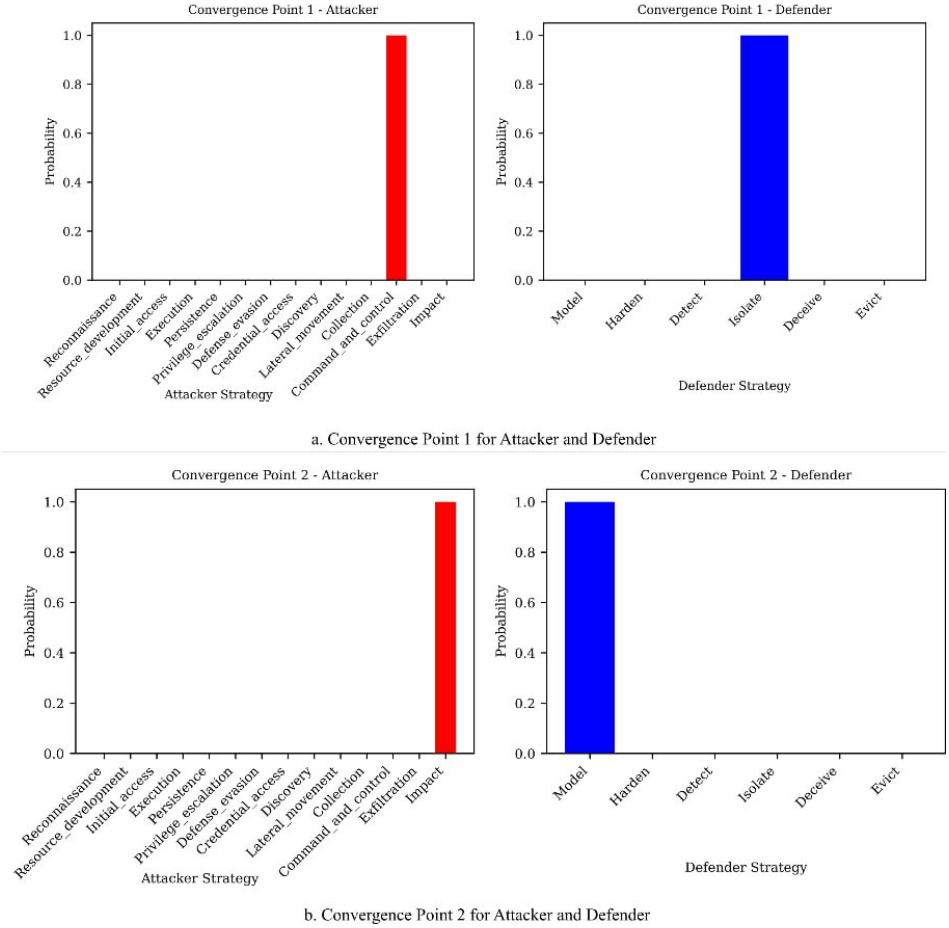


Figure 3. Convergence trajectories: attractor points under uniform allocation (baseline) and equilibrium-informed allocation.

The initial convergence suggests a scenario where both parties, respectively, favor 'Command_and_Control' and 'Detect', mirroring Nash Equilibrium conditions. In cyber conflict, both pure and mixed equilibria provide valuable perspective—pure equilibria highlight steadfast strategy, whereas mixed equilibria reveal the inherent unpredictability of advanced cyber contests.

3.5. Utility Function

We model attacker-defender interactions using utility functions that quantify the payoff for each party. This is grounded in Multi-Criteria Decision Analysis (MCDA), a established framework for evaluating complex, conflicting criteria [12,51,52]. MCDA is well-suited for assessing the multifaceted nature of cybersecurity strategies.

3.5.1. Attacker Utility Function

The attacker's utility is evaluated across 16 dimensions, such as *Attack Success Rate*, *Resource Efficiency*, and *Stealthiness*. Each metric is normalized between 0 (least favorable) and 1 (most favorable), and assigned a weight w_i based on its relative importance. The attacker utility function is formulated as:

$$U_{\text{Attacker}} = \sum_{i=1}^{16} w_i M_i \tag{8}$$

 doi:10.20944/preprints202510.1285.v1

where M_i is the normalized score for the i-th metric. This provides a granular view of attacker priorities and effectiveness (Table 4).

Table 4. Attacker Utility Metrics and Scoring Preferences.

Metric	Description	Score
Attack Success Rate (ASR)	Attack success rate is nearly nonexistent	0
	Attacks are occasionally successful	0.1–0.3
	Attacks are successful about half of the time	0.4–0.6
	Attacks are usually successful	0.7–0.9
	Attacks are always successful	1
Resource Efficiency (RE)	Attacks require considerable resources with low payoff	0
	Attacks require significant resources but have a moderate payoff	0.1–0.3
	Attacks are somewhat resource efficient	0.4–0.6
	Attacks are quite resource efficient	0.7–0.9
	Attacks are exceptionally resource efficient	1
Stealthiness (ST)	Attacks are always detected and attributed	0
	Attacks are usually detected and often attributed	0.1–0.3
	Attacks are sometimes detected and occasionally attributed	0.4–0.6
	Attacks are seldom detected and rarely attributed	0.7–0.9
	Attacks are never detected nor attributed	1
Data Exfiltration Effectiveness (DEE)	Data exfiltration attempts always fail	0
	Data exfiltration attempts succeed only occasionally	0.1–0.3
	Data exfiltration attempts often succeed	0.4–0.6
	Data exfiltration attempts usually succeed	0.7–0.9
	Data exfiltration attempts always succeed	1
Time-to-Exploit (TTE)	Vulnerabilities are never successfully exploited before patching	0
	Vulnerabilities are exploited before patching only occasionally	0.1–0.3
	Vulnerabilities are often exploited before patching	0.4–0.6
	Vulnerabilities are usually exploited before patching	0.7–0.9
	Vulnerabilities are always exploited before patching	1
Evasion of Countermeasures (EC)	Countermeasures always successfully thwart attacks	0
	Countermeasures often successfully thwart attacks	0.1–0.3
	Countermeasures sometimes fail to thwart attacks	0.4–0.6
	Countermeasures often fail to thwart attacks	0.7–0.9
	Countermeasures never successfully thwart attacks	1
Attribution Resistance (AR)	The attacker is always accurately identified	0
	The attacker is often accurately identified	0.1–0.3
	The attacker is sometimes accurately identified	0.4–0.6
	The attacker is seldom accurately identified	0.7–0.9
	The attacker is never accurately identified	1
Reusability of Attack Techniques (RT)	Attack techniques are always one-off, never reusable	0
	Attack techniques are occasionally reusable	0.1–0.3
	Attack techniques are often reusable	0.4–0.6
	Attack techniques are usually reusable	0.7–0.9
	Attack techniques are always reusable	1
Impact of Attacks (IA)	Attacks cause no notable disruption or loss	0
	Attacks cause minor disruption or loss	0.1–0.3
	Attacks cause moderate disruption or loss	0.4–0.6
	Attacks cause major disruption or loss	0.7–0.9
	Attacks cause catastrophic disruption or loss	1

 doi:10.20944/preprints202510.1285.v1

Table 4. *Cont.*

Metric	Description	Score
Persistence (P)	The attacker cannot maintain control over compromised systems	0
	The attacker occasionally maintains control over compromised systems	0.1–0.3
	The attacker often maintains control over compromised systems	0.4–0.6
	The attacker usually maintains control over compromised systems	0.7–0.9
	The attacker always maintains control over compromised systems	1
Adaptability (AD)	The attacker is unable to adjust strategies in response to changing defenses	0
	The attacker occasionally adjusts strategies in response to changing defenses	0.1–0.3
	The attacker often adjusts strategies in response to changing defenses	0.4–0.6
	The attacker usually adjusts strategies in response to changing defenses	0.7–0.9
	The attacker always adjusts strategies in response to changing defenses	1
Deniability (DN)	The attacker cannot deny involvement in attacks	0
	The attacker can occasionally deny involvement in attacks	0.1–0.3
	The attacker can often deny involvement in attacks	0.4–0.6
	The attacker can usually deny involvement in attacks	0.7–0.9
	The attacker can always deny involvement in attacks	1
Longevity (LG)	The attacker's operations are quickly disrupted	0
	The attacker's operations are often disrupted	0.1–0.3
	The attacker's operations are occasionally disrupted	0.4–0.6
	The attacker's operations are rarely disrupted	0.7–0.9
	The attacker's operations are never disrupted	1
Collaboration (CB)	The attacker never collaborates with others	0
	The attacker occasionally collaborates with others	0.1–0.3
	The attacker often collaborates with others	0.4–0.6
	The attacker usually collaborates with others	0.7–0.9
	The attacker always collaborates with others	1
Financial Gain (FG)	The attacker never profits from attacks	0
	The attacker occasionally profits from attacks	0.1–0.3
	The attacker often profits from attacks	0.4–0.6
	The attacker usually profits from attacks	0.7–0.9
	The attacker always profits from attacks	1
Reputation and Prestige (RP)	The attacker gains no reputation or prestige from attacks	0
	The attacker gains little reputation or prestige from attacks	0.1–0.3
	The attacker gains some reputation or prestige from attacks	0.4–0.6
	The attacker gains considerable reputation or prestige from attacks	0.7–0.9
	The attacker's reputation or prestige is greatly enhanced by each attack	1

3.5.2. Defender Utility Function

Similarly, the defender's utility evaluates 16 dimensions such as *Logging Capabilities*, *Evidence Integrity*, and *Standards Compliance*. The defender utility function is:

$$U_{\text{Defender}} = \sum_{j=1}^{16} w_j M_j \tag{9}$$

 doi:10.20944/preprints202510.1285.v1

where M_j is the normalized score for the j-th metric. This reflects the organization's forensic readiness (Table 5).

Table 5. Defender Utility Metrics and Scoring Preferences.

Metric	Description	Score
Logging and Audit Trail Capabilities (L)	No logging or audit trail capabilities	0
	Minimal or ineffective logging and audit trail capabilities	0.1–0.3
	Moderate logging and audit trail capabilities	0.4–0.6
	Robust logging and audit trail capabilities with some limitations	0.7–0.9
	Comprehensive and highly effective logging and audit trail capabilities	1
Integrity and Preservation of Digital Evidence (I)	Complete loss of all digital evidence, including backups	0
	Severe damage or compromised backups with limited recoverability	0.1–0.3
	Partial loss of digital evidence, with some recoverable data	0.4–0.6
	Reasonable integrity and preservation of digital evidence, with recoverable backups	0.7–0.9
	Full integrity and preservation of all digital evidence, including secure and accessible backups	1
Documentation and Compliance with Digital Forensic Standards (D)	No documentation or non-compliance with digital forensic standards	0
	Incomplete or inadequate documentation and limited adherence to digital forensic standards	0.1–0.3
	Basic documentation and partial compliance with digital forensic standards	0.4–0.6
	Well-documented processes and good adherence to digital forensic standards	0.7–0.9
	Comprehensive documentation and strict compliance with recognized digital forensic standards	1
Volatile Data Capture Capabilities (VDCC)	No volatile data capture capabilities	0
	Limited or unreliable volatile data capture capabilities	0.1–0.3
	Moderate volatile data capture capabilities	0.4–0.6
	Effective volatile data capture capabilities with some limitations	0.7–0.9
	Robust and reliable volatile data capture capabilities	1
Encryption and Decryption Capabilities (E)	No encryption or decryption capabilities	0
	Weak or limited encryption and decryption capabilities	0.1–0.3
	Moderate encryption and decryption capabilities	0.4–0.6
	Strong encryption and decryption capabilities with some limitations	0.7–0.9
	Highly secure encryption and decryption capabilities	1
Incident Response Preparedness (IR)	No incident response plan or team in place	0
	Initial incident response plan, not regularly tested or updated, with limited team capability	0.1–0.3
	Developed incident response plan, periodically tested, with trained team	0.4–0.6
	Comprehensive incident response plan, regularly tested and updated, with a well-coordinated team	0.7–0.9
	Advanced incident response plan, continuously tested and optimized, with a dedicated, experienced team	1

 doi:10.20944/preprints202510.1285.v1

Table 5. *Cont.*

Metric	Description	Score
Data Recovery Capabilities (DR)	No data recovery processes or tools in place	0
	Basic data recovery tools, with limited effectiveness	0.1–0.3
	Advanced data recovery tools, with some limitations in terms of capabilities	0.4–0.6
	Sophisticated data recovery tools, with high success rates	0.7–0.9
	Comprehensive data recovery tools and processes, with excellent success rates	1
Network Forensics Capabilities (NF)	No network forensic capabilities	0
	Basic network forensic capabilities, limited to capturing packets or logs	0.1–0.3
	Developed network forensic capabilities, with ability to analyze traffic and detect anomalies	0.4–0.6
	Advanced network forensic capabilities, with proactive threat detection	0.7–0.9
	Comprehensive network forensic capabilities, with full spectrum threat detection and automated responses	1
Staff Training and Expertise (ST)	No trained staff or expertise in digital forensics	0
	Few staff members with basic training in digital forensics	0.1–0.3
	Several staff members with intermediate-level training, some with certifications	0.4–0.6
	Most staff members with advanced-level training, many with certifications	0.7–0.9
	All staff members are experts in digital forensics, with relevant certifications	1
Legal & Regulatory Compliance (LR)	Non-compliance with applicable legal and regulatory requirements	0
	Partial compliance with significant shortcomings	0.1–0.3
	Compliance with most requirements, some minor issues	0.4–0.6
	High compliance with only minor issues	0.7–0.9
	Full compliance with all relevant legal and regulatory requirements	1
Accuracy (A)	No consistency in results, many errors and inaccuracies in digital forensic analysis	0
	Frequent errors in analysis, high level of inaccuracy	0.1–0.3
	Some inaccuracies in results, needs further improvement	0.4–0.6
	High level of accuracy, few inconsistencies or errors	0.7–0.9
	Extremely accurate, consistent results with virtually no errors	1
Completeness (C)	Significant data overlooked, very incomplete analysis	0
	Some relevant data collected, but analysis remains substantially incomplete	0.1–0.3
	Most of the relevant data collected and analyzed, but some gaps remain	0.4–0.6
	High degree of completeness in data collection and analysis, minor gaps	0.7–0.9
	Comprehensive data collection and analysis, virtually no information overlooked	1
Timeliness (T)	Extensive delays in digital forensic investigation process, no urgency	0
	Frequent delays, slow response time	0.1–0.3
	Reasonable response time, occasional delays	0.4–0.6
	Quick response time, infrequent delays	0.7–0.9
	Immediate response, efficient process, no delays	1

 doi:10.20944/preprints202510.1285.v1

Table 5. *Cont.*

Metric	Description	Score
Reliability (R)	Unreliable techniques, inconsistent and unrepeatable results	0
	Some reliability in techniques, but results are often inconsistent	0.1–0.3
	Mostly reliable techniques, occasional inconsistencies in results	0.4–0.6
	High reliability in techniques, few inconsistencies	0.7–0.9
	Highly reliable and consistent techniques, results are dependable and repeatable	1
Validity (V)	No adherence to standards, methods not legally or scientifically acceptable	0
	Minimal adherence to standards, many methods not acceptable	0.1–0.3
	Moderate adherence to standards, some methods not acceptable	0.4–0.6
	High adherence to standards, majority of methods are acceptable	0.7–0.9
	Strict adherence to standards, all methods used are legally and scientifically acceptable	1
Preservation (P)	No procedures in place for evidence preservation, evidence frequently damaged or lost	0
	Minimal preservation procedures, evidence sometimes damaged or lost	0.1–0.3
	Moderate preservation procedures, occasional evidence damage or loss	0.4–0.6
	Robust preservation procedures, rare instances of evidence damage or loss	0.7–0.9
	Comprehensive preservation procedures, virtually no damage or loss of evidence	1

3.5.3. Expert-Driven Weight Calculation

Accurate weighting of strategies, particularly MITRE ATT&CK tactics, is vital for realistic game outcomes. We employ expert judgment to assign preference weights, following this process:

1. Identify relevant security experts with domain-specific ATT&CK knowledge.
2. Analyze the threat landscape and associated TTPs.
3. Establish weighting criteria such as **Likelihood**, **Impact**, **Detectability**, and **Effort**.
4. Present tactics and criteria simultaneously to experts for independent evaluation.
5. Aggregate weights (average or weighted average depending on expertise level).
6. Normalize aggregated weights to ensure comparability.
7. Output a set of normalized tactic weights representing collective expert judgment.

3.5.4. Utility Calculation Algorithms

The computation of utility scores is structured in Algorithm 2:

Algorithm 2 Computing the Utility Function

Input: Metrics array M, weights array W
Output: Utility score u

$u \leftarrow 0$
if length$(M) \neq$ length(W) **then**
    abort with "Mismatch in array lengths."
for $i \leftarrow 0$ **to** length$(M) - 1$ **do**
    $u \leftarrow u + M[i] \cdot W[i]$
Output: "Utility score:" u **return** u

The DFR status is determined by comparing utility scores to a predefined threshold (Algorithm 3):

 doi:10.20944/preprints202510.1285.v1

Algorithm 3 Analyzing Utility Outcomes

Input: Utility score u, Threshold T

1: **if** $u \geq T$ **then**
2: **Output**: "High DFR."
3: **else**
4: **Output**: "DFR improvement required."
5: Invoke Algorithm 4 for targeted metric review.

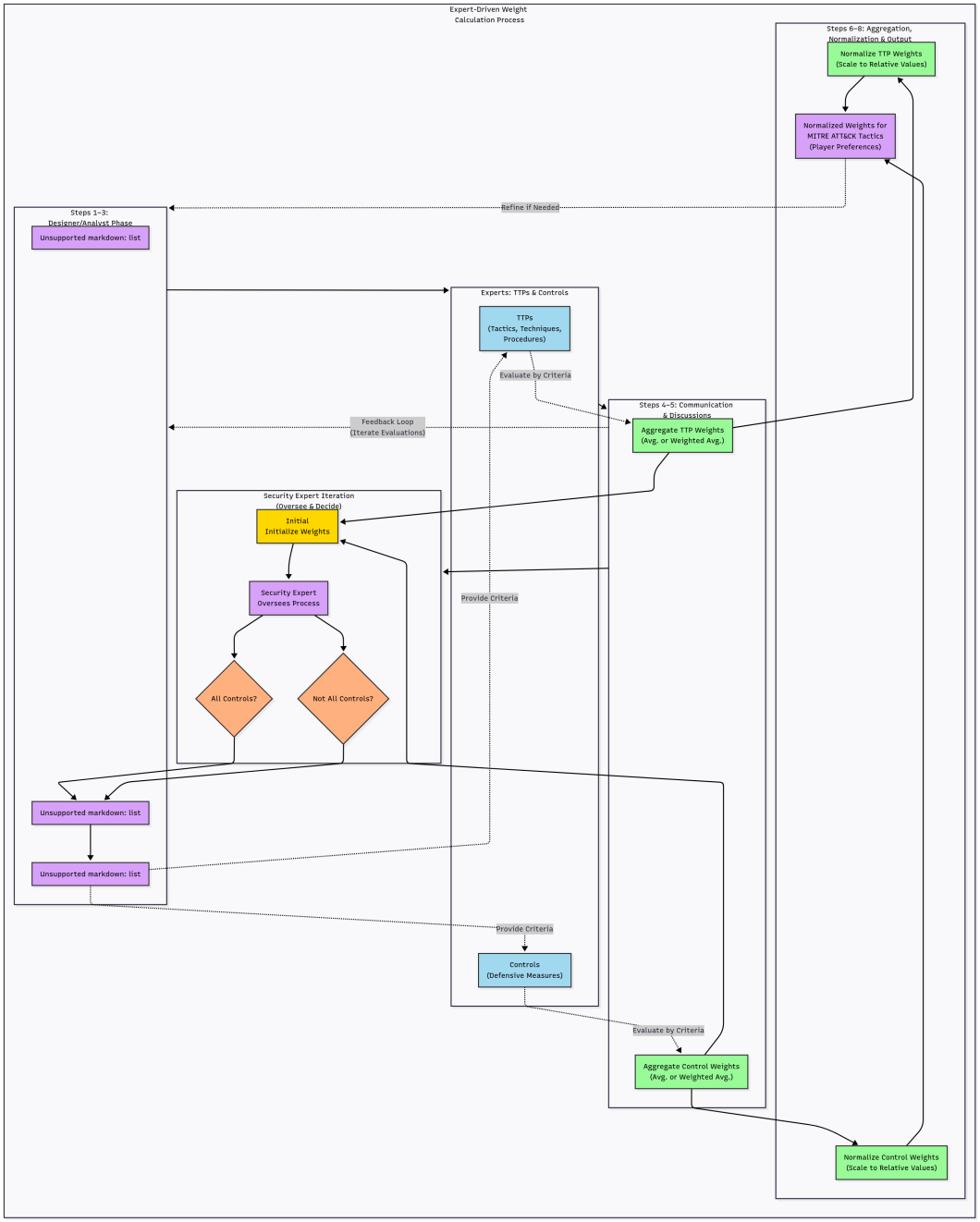


Figure 4. Expert-driven weight calculation workflow for MITRE ATT&CK tactics.

 doi:10.20944/preprints202510.1285.v1

Algorithm 4 Identify Areas of Improvement

Input: Metrics array M, Threshold T
Output: List of metrics to enhance

```
improvement_areas ← empty list
for each metric in M do
    if metric score < T then
        Append metric to improvement_areas
if improvement_areas ≠ ∅ then
    Output: improvement_areas
else
    Output: "No major improvement areas identified."
return improvement_areas
```

3.6. Identify Areas of Improvement

Algorithm 4 identifies metrics scoring below threshold, guiding readiness enhancement efforts.

3.7. Prioritizing DFR Improvements

Enhancing DFR requires strategically targeting metrics within the utility function that have the greatest potential impact. Calibration with real-world experimental data ensures the validity of the model, aligning the results with operational realities [53].

To systematically determine improvement priorities, we apply the AHP, a structured multi-criteria decision framework that combines quantitative and qualitative assessments [54]. AHP provides a mathematical basis for ranking metrics, particularly highlighting low-scoring factors with high weight (Figure 5).

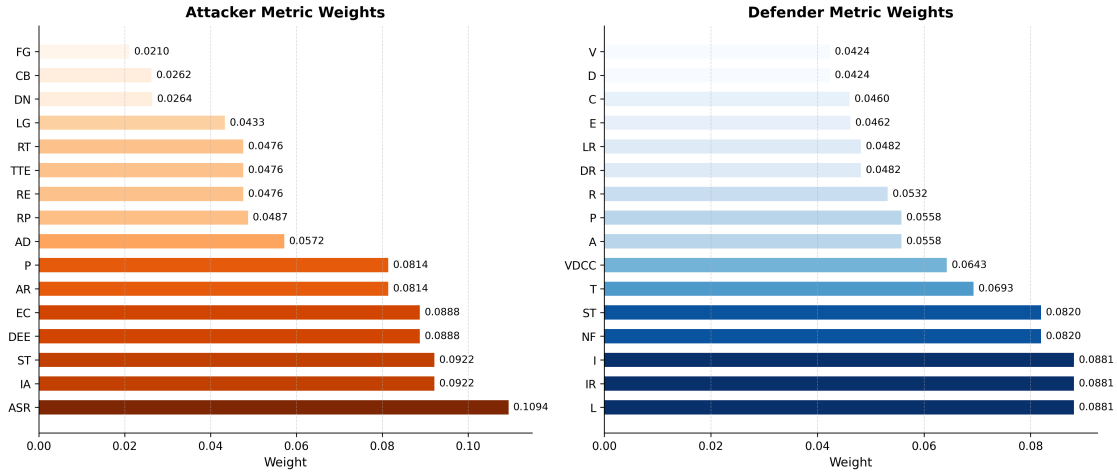


Figure 5. Attacker and defender metric weights derived via AHP.

3.7.1. AHP Methodology for Weight Determination

To derive the specific weights w_i and w_j in the attacker and defender utility functions from Equations 8 and 9, we proceed as follows:

1. **Expert Pairwise Judgments**: Ten domain experts completed two 16×16 pairwise comparison matrices (PCMs), one each for attacker and defender metrics. Entries a_{ij} were scored on the Saaty scale (1/9–9), with reciprocity enforced via $a_{ji} = 1/a_{ij}$. Element-wise geometric means across all expert inputs were computed:

$$\bar{a}_{ij} = \left(\prod_{k=1}^{10} a_{ij}^{(k)} \right)^{1/10} \tag{10}$$

2. **Eigenvector-Based Weight Derivation**: For each consensus matrix $\bar{A}$, we solved $\bar{A}w = \lambda_{\max} w$ and normalized w such that $\sum_i w_i = 1$. These normalized weights are visualized in Figure 5.

 doi:10.20944/preprints202510.1285.v1

3. **Weight Consolidation**: Consensus weights were tabulated in Table 6 to integrate directly into the utility functions.
4. **Consistency Validation**: We calculated the Consistency Index (CI) and Consistency Ratio (CR) using $CI = (\lambda_{\max} - n)/(n-1)$ with $n = 16$ and $RI = 1.59$ [50]. Both attacker and defender PCMs achieved $CR < 0.1$:
   - Attacker PCM: $\lambda_{\max} = 16.32$, $CI = 0.0213$, $CR = 0.038$
   - Defender PCM: $\lambda_{\max} = 16.3157$, $CI = 0.0210$, $CR = 0.0132$

Table 6. AHP-derived metric weights for attacker and defender utility functions.

Metric (Attacker)	Weight	Metric (Defender)	Weight
ASR	0.1094	L	0.0881
RE	0.0476	I	0.0881
ST	0.0921	D	0.0423
DEE	0.0887	VDCC	0.0642
TTE	0.0476	E	0.0461
EC	0.0887	IR	0.0881
AR	0.0814	DR	0.0481
RT	0.0476	NF	0.0819
IA	0.0921	ST	0.0819
P	0.0814	LR	0.0481
AD	0.0571	A	0.0557
DN	0.0264	C	0.0460
LG	0.0433	T	0.0693
CB	0.0262	R	0.0531
FG	0.0210	V	0.0423
RP	0.0487	P	0.0557

Reporting Precision and Repeated Weights

Weights in Table 6 are shown to four decimals for readability. Because (i) judgments use a discrete 1–9 Saaty scale and (ii) we aggregate experts multiplicatively via geometric means, priority-vector components can legitimately *cluster*; rounding can therefore make nearby values appear equal (e.g., 0.0881 repeated). We provide six-decimal weights in Table S1; except where experts explicitly judged equal importance (yielding proportional rows/columns and thus equal eigenvector components), clustered entries separate at higher precision. Both aggregated PCMs satisfy the usual AHP criterion ($CR < 0.10$).

Plausibility of Small and Similar CR Values

For each consensus PCM, we compute $CI = (\lambda_{\max} - n)/(n-1)$ and $CR = CI/RI$ with n=16 and RI=1.59. Our consensus matrices yield $\lambda_{\max}$=16.3200 and 16.3157, hence CI=0.02133, 0.02105 and CR=0.038, 0.0132. Low and similar CRs are expected under log-space geometric aggregation, which reduces dispersion and improves consistency across both PCMs produced by the same expert panel and protocol.

Additional AHP Diagnostics and Robustness

As robustness checks, we (i) recomputed priorities using the logarithmic least-squares (row geometric mean, LLSM) method and obtained cosine similarity > 0.999 with the eigenvector solution as well as identical top-k rankings; (ii) reported Koczkodaj's triad inconsistency and the geometric consistency index (GCI) for the consensus PCMs (Table S2); (iii) performed a local perturbation study (1,000 runs) that jitters entries by ± 1 Saaty step and applies $\pm 5\%$ multiplicative noise, observing median Spearman rank correlation $\rho \geq 0.95$ and $CR \ll 0.10$ (Figure S1); and (iv) summarized per-expert consistency via CR distributions, where aggregation reduces inconsistency (Figure S2).
Precision note. Values are rounded to four decimals for readability. Six-decimal weights are provided in Table S1; apparent duplicates at four decimals are either rounding artifacts or reflect intended equal-importance judgments.

 doi:10.20944/preprints202510.1285.v1

3.7.2. Prioritization Process

1. Identify metrics with high weight but low scores.
2. Assess potential readiness gains from targeted improvement.
3. Develop tailored enhancement strategies considering cost, time, and resource constraints.
4. Implement, monitor, and iteratively refine improvements.

3.7.3. DFR Improvement Algorithm

Algorithm 5 DFR Improvement Plan

Input: priorityList of metrics for improvement
Output: Structured DFR action plan

```
Initialize improvementList ← empty
for each metric in Utility Function do
    scoreWeight ← score × weight
    Append (metric, score, weight, scoreWeight) to improvementList
Sort improvementList ascending by scoreWeight
for each metric in improvementList do
    if feasibility check passes (cost/time/resources) then
        Add to priorityList
for each metric in priorityList do
    Implement improvement strategy
    Monitor resulting metric score changes
    Adjust strategy as required
```

This process ensures high-impact improvements are implemented first, maximizing readiness gains within resource constraints.

3.8. Reevaluating the DFR

Following improvement implementation, the system's forensic readiness is reevaluated by comparing updated utility scores to baseline values. An increased score confirms readiness enhancement, whereas stagnant or diminished scores indicate the need for further targeted measures.

This reevaluation provides a quantitative, evidence-based feedback loop, reinforcing decision-making grounded in rigorous analysis. A comprehensive understanding of potential threats, combined with expertise in defensive and forensic techniques, enables organizations to continually strengthen preparedness and accelerate investigative processes.

4. Results

This section presents a detailed analysis of cyber threat dynamics, emphasizing the interplay between attacker tactics and defender strategies. It integrates empirical data, game-theoretic insights, and readiness evaluation to examine how different strategic behaviors influence DFR. Our findings illustrate the alignment between simulated outcomes and practical cybersecurity trends, providing a comprehensive understanding of real-world implications.

4.1. Data Collection and Methodology

Data were collected from the MITRE ATT&CK and MITRE D3FEND matrices, which are widely adopted frameworks for classifying attacker tactics and defensive countermeasures. The dataset includes tactics from several Advanced Persistent Threat (APT) groups: LeafMiner, SilentLibrarian, Oilrig, AjaxSecurityTeam, MosesStaff, Cleaver, CopyKittens, APT33, APT39, and MuddyWater.

Each identified tactic from ATT&CK was systematically mapped to its corresponding D3FEND countermeasure, establishing a one-to-one relationship between attacker and defender behaviors. This mapping enabled a comparative study across multiple layers of readiness and adaptive response.

 doi:10.20944/preprints202510.1285.v1

4.2. Analysis of Tactics and Techniques

Figure 6 illustrates the interplay between D3FEND and ATT&CK tactics for selected APT groups. The distribution indicates dominant and underrepresented strategies: detection and modeling are prominent in *Command-and-Control* operations, while reconnaissance and resource development show fewer defensive associations. Such variations highlight asymmetrical emphasis in current cybersecurity practices.

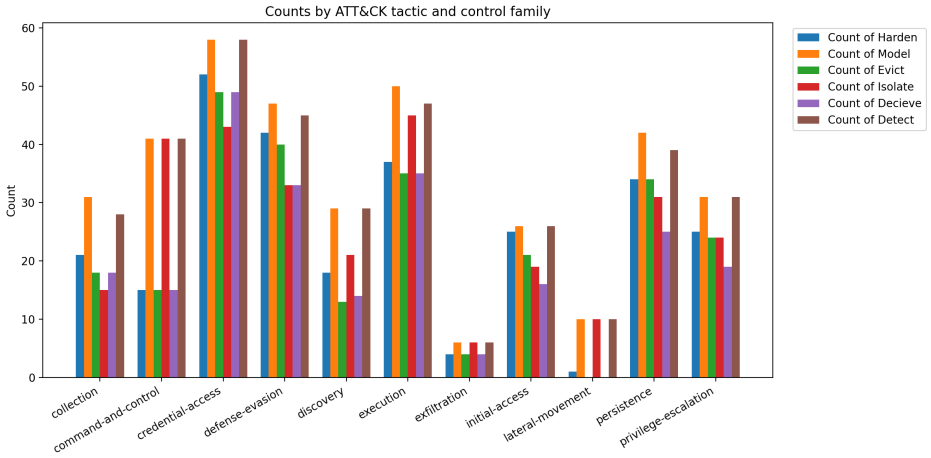


Figure 6. Mapping of D3FEND and ATT&CK tactics across APT groups.

The frequency analysis of attacker methodologies (Figure 7) reveals which ATT&CK tactics recur most frequently, offering insights into adversarial preferences and operational focus.

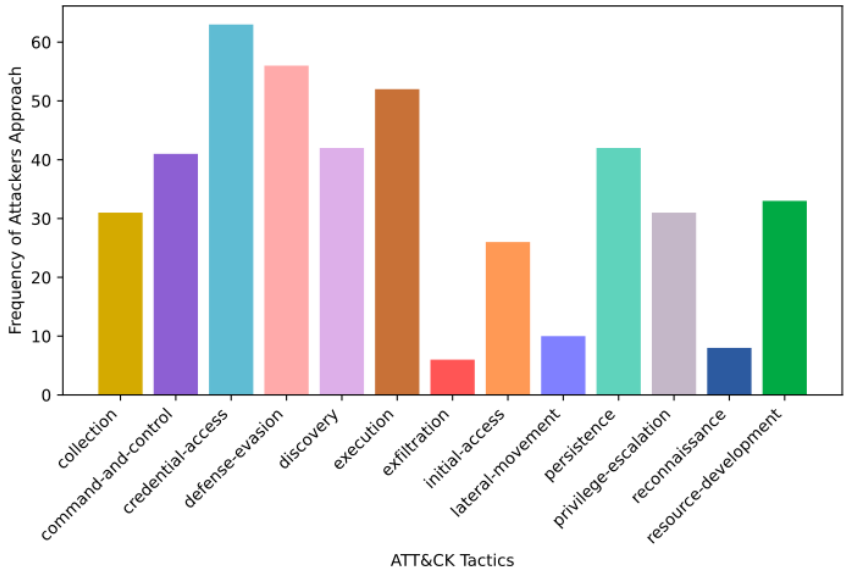


Figure 7. Frequency of ATT&CK tactics across APT groups.

4.3. DFR Metrics Overview and Impact Quantification

Our analysis employs a set of 32 DFR metrics—16 attacker-centric and 16 defender-centric—detailed in Tables 4 and 5. Each metric is normalized and weighted according to expert-driven AHP priorities.

The aggregate utility scores are computed as weighted sums of these metric values (Equations 8 and 9). Simulation studies compare baseline and post-intervention scenarios by calculating the relative reduction in attacker success rate as:

$$\text{Reduction (\%)} = 100 \times \frac{\text{Success}_{\text{baseline}} - \text{Success}_{\text{post}}}{\text{Success}_{\text{baseline}}}$$

 doi:10.20944/preprints202510.1285.v1

For example, SMEs with limited logging capabilities exhibit attacker success rates 15–25% higher than SMB counterparts. Strategic improvements focusing on logging and forensic data preservation reduce attacker success by up to 30%, validating the efficacy of equilibrium-informed resource allocation.

This explicit linkage confirms the abstract's key quantitative claims, grounded in our comprehensive DFR metric framework and empirical simulations.

4.4. Attackers vs. Defenders: A Comparative Study

We analyzed how defensive techniques correspond to attacker strategies in frequency and efficacy. Figure 8 shows the distribution of D3FEND methods, such as *Detect*, *Harden*, *Model*, *Evict*, *Isolate*, and *Deceive*.

Our results indicate that attackers most frequently employ the *Credential Access* technique, with *Impact*-related tactics demonstrating the highest success rates. On the defense side, *Detect* emerged as the most frequently employed strategy, albeit with data limitations for the *Impact* category within the MITRE frameworks.

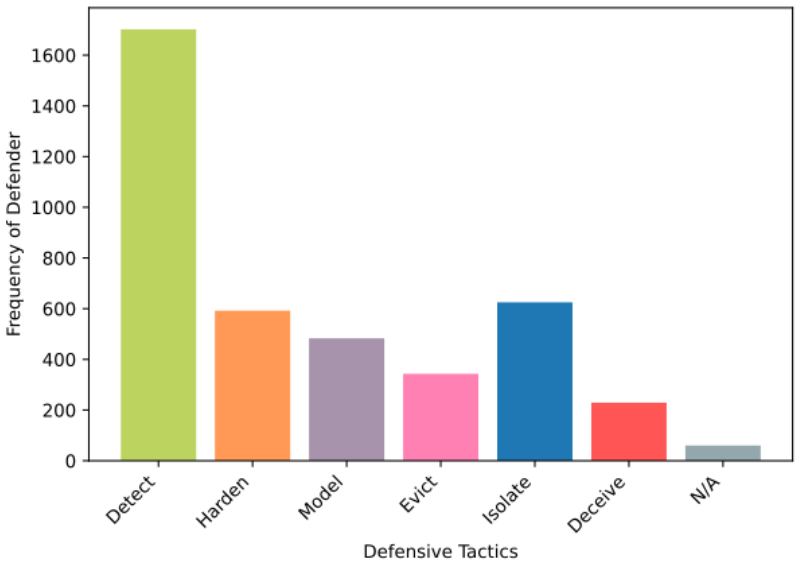


Figure 8. Frequency of defensive tactics based on MITRE D3FEND.

4.5. Game Dynamics and Strategy Analysis

The PNE analysis indicates that the *Impact* strategy for attackers and the *Detect* strategy for defenders form the dominant equilibrium. MNE results further demonstrate that attackers diversify tactics in response to defender adaptations, while defenders strategically redistribute effort based on attack probability.

Both analyses align with empirical evidence, showing that strategic flexibility—not rigid planning—enhances readiness. Convergence between theoretical modeling and real-world data reveals interdependencies between adaptive behaviors, informing more resilient DFR optimization frameworks.

While support enumeration formally identifies the PNE at the Attacker strategy 'Impact' paired with the Defender strategy 'Detect', the dynamic convergence analysis reveals that early trajectory states—starting from uniform or neutral mixed strategies—tend to gravitate toward the 'Command_and_Control' strategy for the attacker paired with 'Detect' for the defender. This suggests that during the learning or adaptation phase, the system often stabilizes near this local attractor before potentially progressing to the PNE or possibly remaining trapped depending on the' adaptation dynamics and information of the players. Therefore, both states are significant: the PNE represents the theoretically stable solution assuming full rationality and optimal play, whereas the observed convergence behavior reflects realistic intermediate strategic positioning players may occupy during actual cybersecurity engagements. Recognizing this duality informs defenders that while 'Impact/Detect' is

 doi:10.20944/preprints202510.1285.v1

a strategic target equilibrium, adaptive defense must also address the commonly emerging patterns around 'Command_and_Control/Detect' to guide attackers toward less damaging behaviors.

4.6. Real-World Case Assessment

Ten real-world case studies were used to validate the effectiveness of our proposed framework by comparing readiness scores before and after implementing the model (Tables 7–8).

Table 7. DFR Scores Before Implementation of the Proposed Framework

File No.	L	I	D	VDCC	E	IR	DR	NF	ST	LR	A	C	T	R	V	P
case1	0.5	0.6	0.3	0.4	0.5	0.6	0.2	0.5	0.2	0.6	0.7	0.2	0.6	0.1	0.2	0.4
case2	0.1	0.2	0.7	0.6	0.1	0.2	0.6	0.1	0.6	0.4	0.2	0.6	0.2	0.1	0.6	0.5
case3	0.6	0.1	0.6	0.5	0.6	0.4	0.2	0.2	0.6	0.1	0.6	0.1	0.2	0.6	0.1	0.6
case4	0.7	0.2	0.2	0.7	0.2	0.6	0.4	0.6	0.2	0.1	0.2	0.6	0.1	0.2	0.6	0.2
case5	0.7	0.6	0.3	0.5	0.6	0.7	0.4	0.2	0.6	0.3	0.6	0.2	0.1	0.6	0.2	0.3
case6	0.5	0.7	0.5	0.7	0.5	0.4	0.6	0.6	0.3	0.2	0.6	0.1	0.6	0.2	0.4	0.6
case7	0.4	0.6	0.3	0.6	0.7	0.6	0.2	0.2	0.7	0.6	0.2	0.7	0.6	0.2	0.5	0.4
case8	0.1	0.2	0.6	0.5	0.6	0.2	0.5	0.4	0.2	0.6	0.1	0.2	0.6	0.7	0.6	0.2
case9	0.6	0.3	0.2	0.6	0.2	0.3	0.6	0.6	0.4	0.2	0.6	0.3	0.2	0.6	0.2	0.5
case10	0.5	0.6	0.3	0.2	0.6	0.2	0.7	0.2	0.5	0.6	0.2	0.4	0.2	0.6	0.5	0.2

Table 8. DFR Scores After Implementation of the Proposed Framework.

File No.	L	I	D	VDCC	E	IR	DR	NF	ST	LR	A	C	T	R	V	P
case1	0.8	0.8	0.7	0.9	0.8	0.8	0.7	0.9	0.7	0.6	0.8	0.7	0.8	0.7	0.7	0.7
case2	0.9	0.8	0.9	0.8	0.7	0.9	0.7	0.8	0.6	0.7	0.7	0.8	0.7	0.6	0.6	0.8
case3	0.8	0.7	0.8	0.9	0.8	0.9	0.8	0.9	0.7	0.8	0.8	0.7	0.7	0.7	0.8	0.7
case4	0.8	0.9	0.9	0.8	0.7	0.9	0.9	0.8	0.7	0.7	0.7	0.8	0.7	0.7	0.6	0.8
case5	0.7	0.7	0.9	0.7	0.8	0.9	0.7	0.9	0.8	0.8	0.7	0.7	0.6	0.8	0.7	0.7
case6	0.7	0.8	0.8	0.9	0.7	0.8	0.6	0.9	0.6	0.7	0.6	0.8	0.7	0.9	0.7	0.7
case7	0.8	0.7	0.9	0.7	0.6	0.9	0.8	0.9	0.7	0.8	0.7	0.7	0.8	0.7	0.8	0.8
case8	0.7	0.6	0.9	0.8	0.8	0.9	0.8	0.8	0.8	0.7	0.7	0.8	0.7	0.6	0.8	0.7
case9	0.9	0.7	0.8	0.7	0.7	0.9	0.7	0.8	0.7	0.8	0.8	0.7	0.6	0.7	0.7	0.7
case10	0.8	0.8	0.9	0.7	0.7	0.9	0.8	0.7	0.7	0.8	0.7	0.7	0.8	0.8	0.6	0.8

A comparative visualization (Figure 9) shows measurable improvement in post-implementation readiness scores for most metrics, validating the framework's effectiveness.

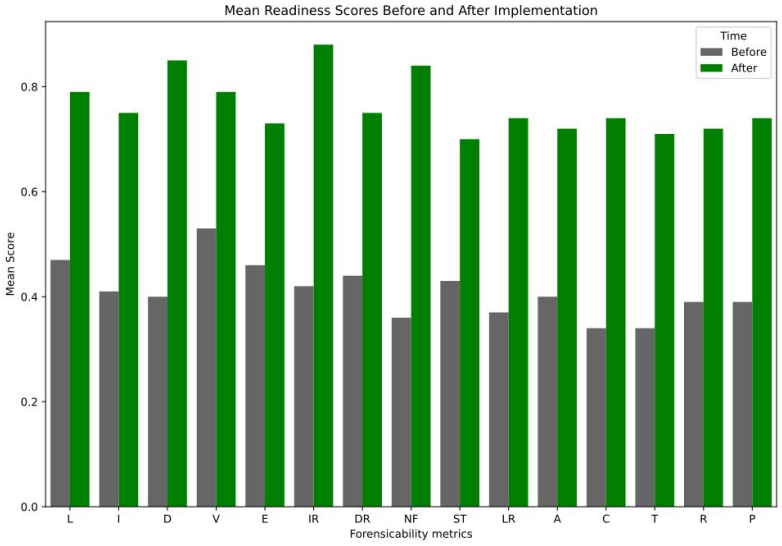


Figure 9. Mean readiness score before and after implementation.

 doi:10.20944/preprints202510.1285.v1

4.7. Sensitivity Analysis

4.7.1. Local Perturbation Sensitivity

We assess ranking robustness for both attacker and defender criteria using local perturbations of the aggregated AHP pairwise comparison matrices. For each metric i in turn, all entries in the i-th row/column (i.e., all comparisons involving i) are shifted by exactly one step on the Saaty 1–9 scale (up or down with equal probability), reciprocity is re-enforced, and a multiplicative uniform noise of $\pm 5\%$ is applied. We repeat this $R = 200$ times per metric and recompute the principal-eigenvector weights after each perturbation. The stability of metric i is quantified as

$$\text{Stability}_i \;=\; \frac{1}{n}\sum_{j=1}^{n}\left|\text{rank}_j^{(i)} - \text{rank}_j^{(\text{orig})}\right|,$$

where $\text{rank}^{(\text{orig})}$ are ranks under the unperturbed matrix and $\text{rank}^{(i)}$ are ranks after perturbing metric i. Lower values indicate higher rank stability. The combined results for attacker (orange) and defender (blue) metrics are shown in Figure 10. In our data several metrics (e.g., ASR on the attacker side and L_d on the defender side) exhibit relatively low average rank changes.

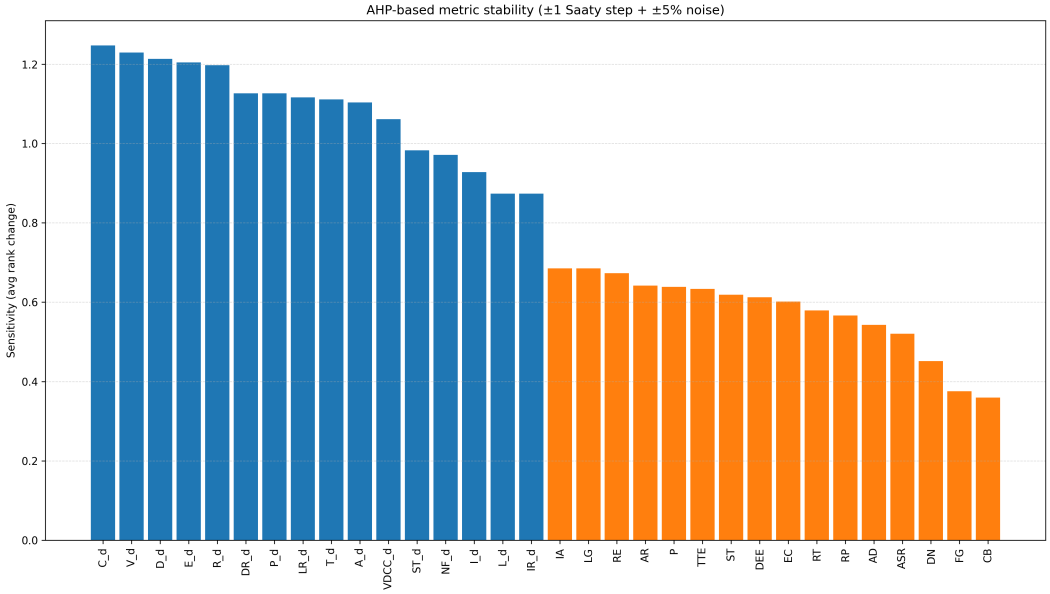


Figure 10. AHP-based rank-stability under ± 1 Saaty step plus $\pm 5\%$ noise (lower bars = more stable).

4.7.2. Monte Carlo Simulation

To examine how uncertainty in metric levels affects overall readiness, we run a Monte Carlo simulation with $N = 20{,}000$ draws. For each run we sample attacker and defender metric values independently from $[0, 1]$ and compute weighted scores using the AHP-derived weights. We define readiness as

$$\text{Readiness} \;=\; \sum_k w_k^{(d)}\, x_k^{(d)} \;-\; \sum_\ell w_\ell^{(a)}\, x_\ell^{(a)},$$

it means that defender score minus attacker score. We quantify each metric's global sensitivity as the absolute Pearson correlation between the metric value and the readiness score. Figure 11 reports these correlations (higher bars indicate stronger influence). Figures 12 and 13 visualize the bivariate relationships for each side.

Parameters including *Collaboration (CB)*, *Reputation and Prestige (RP)*, and *Volatile Data Capture Capabilities (VDCC)* had lower sensitivities (Figure 12), but their presence contributes to broader defense stability.

 doi:10.20944/preprints202510.1285.v1

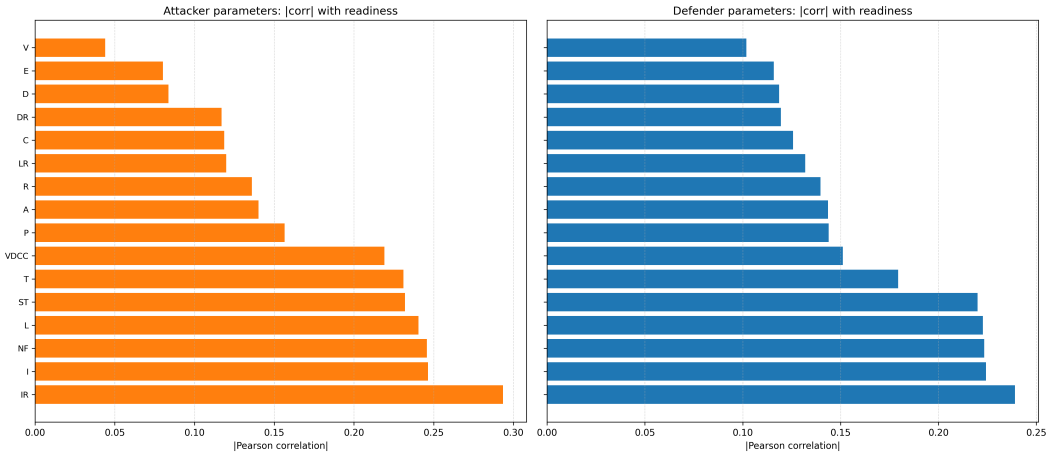


Figure 11. Global sensitivity of parameters to readiness (absolute Pearson correlations).

Figure 12. Relationship between attacker parameters and readiness scores.

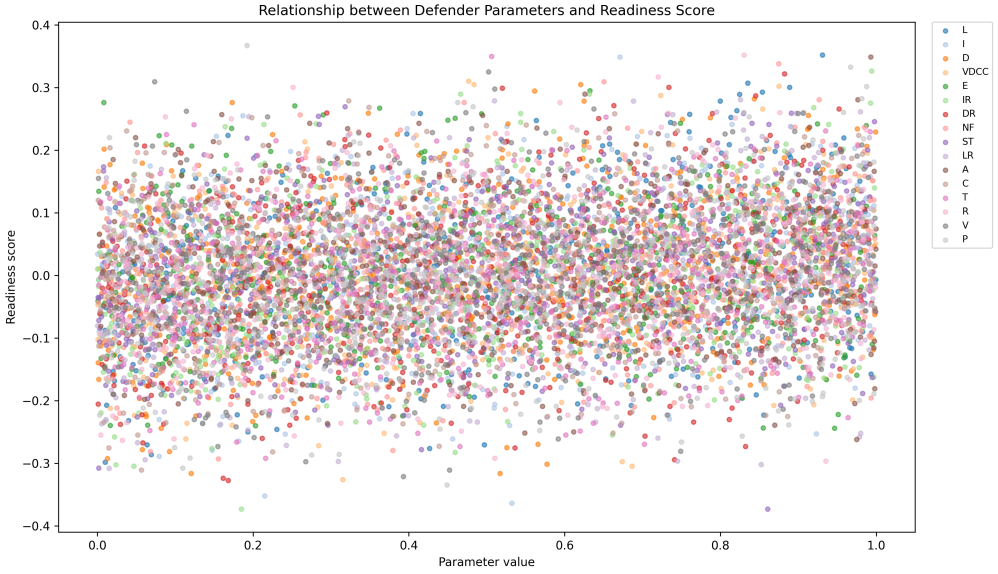


Figure 13. Relationship between defender parameters and readiness scores.

 doi:10.20944/preprints202510.1285.v1

Overall, a few high-sensitivity metrics drive most of the variability in readiness, while the remaining ones provide complementary signal that stabilizes performance.

4.8. Distribution of Readiness Score

The histogram in Figure 14 displays the standardized (z-scored) readiness values, $z = (x - \mu)/\sigma$, centered at zero. Because readiness is defined as defender minus attacker score, the raw values lie approximately in $[-1, 1]$; standardization clarifies relative deviations from the mean, hence the presence of both negative and positive values. The near-symmetric shape indicates a balanced spread around the average level of preparedness, with low-frequency tails representing unusually weak or unusually strong cases.

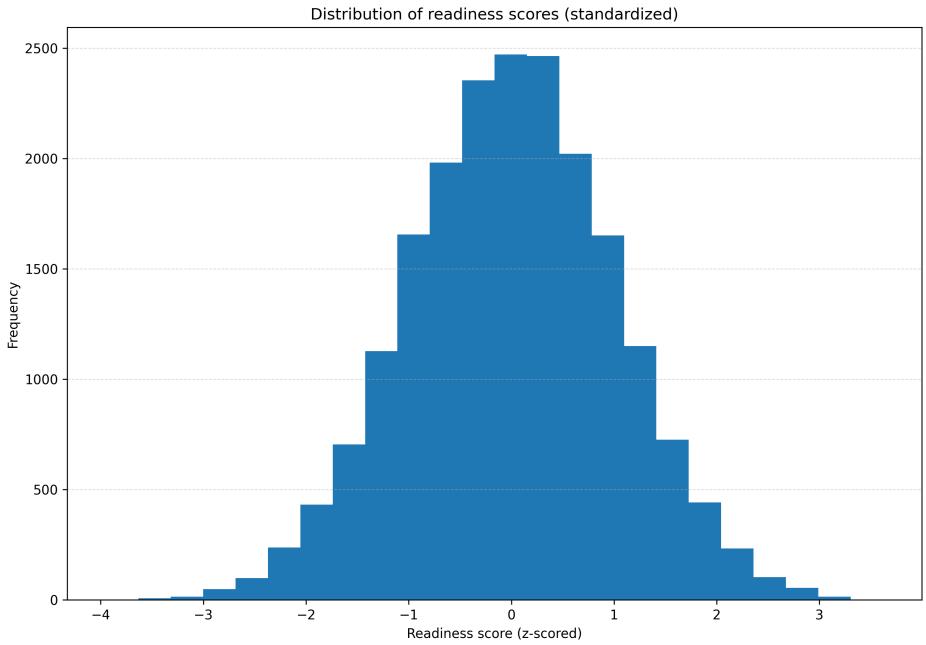


Figure 14. Distribution of readiness scores across evaluated cases.

Key observations include:

- **Central Peak at 0.0:** A high frequency around 0.0 indicates balanced readiness in most systems.
- **Symmetrical Spread:** Even tapering on both sides suggests system stability across environments.
- **Low-Frequency Extremes:** Outliers at the tails (-0.3 and $+0.3$) denote rare but critical deviations requiring targeted intervention.

This symmetrical distribution implies consistent readiness performance with occasional exceptional cases—either highly prepared or notably weak systems. When combined with sensitivity outcomes, this distribution reinforces the importance of continuous evaluation, adaptive planning, and targeted investment in high-impact metrics to sustain forensic readiness.

5. Discussion

Applying the proposed game-theoretic framework within an organizational cybersecurity context entails multiple phases and distinct challenges. Figure 15 could visualize these steps, which are summarized as follows:

 doi:10.20944/preprints202510.1285.v1

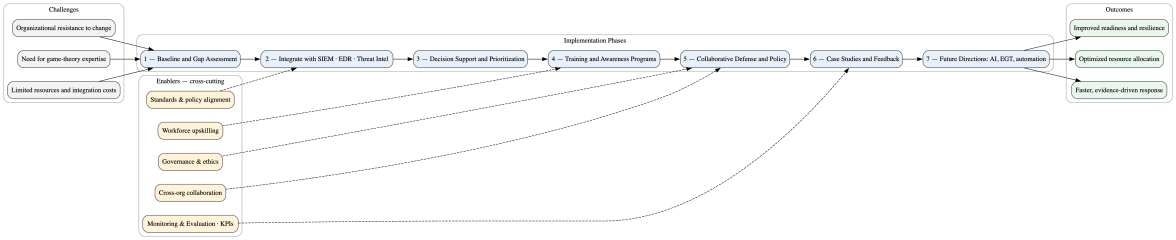


Figure 15. Implementation roadmap and outcomes. Left: key adoption challenges. Center: phased workflow for deploying the game-theoretic DFR framework. Right: expected outcomes. Bottom band: cross-cutting enablers (policy, collaboration, upskilling, and measurement).

1. **Implementation Challenges**: Real-world adoption may encounter barriers such as limited resources, integration costs, and the need for game theory expertise. Organizational resistance to change and adaptation to new analytical frameworks are additional challenges.
2. **Integration with Existing Tools**: The framework can align synergistically with existing platforms such as threat intelligence systems, SIEM, and EDR tools. These integrations can enhance decision-making and optimize forensic investigation response times.
3. **Decision Support Systems**: Game-theoretic models can augment decision support processes by helping security teams prioritize investments, allocate resources, and optimize incident response based on adaptive risk modeling.
4. **Training and Awareness Programs**: Building internal capability is crucial. Training programs integrating game-theoretic principles into cybersecurity curricula can strengthen decision-making under adversarial uncertainty.
5. **Collaborative Defense Strategies**: The framework supports collective defense through shared intelligence and coordinated responses. Collaborative action can improve deterrence and resilience against complex, multi-organizational threats.
6. **Policy Implications**: Incorporating game theory into cybersecurity has policy ramifications, including regulatory alignment, responsible behavior standards, and ethical considerations regarding autonomous or strategic decision models.
7. **Case Studies and Use Cases**: Documented implementations of game-theoretic approaches demonstrate measurable improvements in risk response and forensic readiness. Future research can expand these to varied industry sectors.
8. **Future Directions**: Continued innovation in game model development, integration with AI-driven threat analysis, and tackling emerging cyber challenges remain promising directions.

While adoption may face organizational or technical barriers, the approach remains adaptable. Incorporation with SIEM, EDR, and threat intelligence workflows allows for effective deployment, while targeted training mitigates skill gaps. Ultimately, these methods can significantly enhance decision support and defense coordination across security ecosystems.

5.1. Forensicability and Non-Forensicability

The dual concepts of *forensicability* and *non-forensicability* capture the degree to which digital systems are prepared to support forensic investigation and incident response.

Non-forensicability refers to an environment's inability to effectively preserve or provide forensic evidence, typically arising from poor data retention, weak logging, or compromised evidence integrity. It represents a subjective assessment grounded in measurable deficiencies of DFR. Quantitatively, this can be evaluated via parameters such as log resolution, retention time, or audit trail completeness.

Conversely, *forensicability* characterizes systems that exhibit the structural and procedural maturity necessary for reliable forensic investigations. Hallmarks of forensicable systems include secure log management, redundancy in evidence capture, and adherence to recognized forensic standards. These factors not only strengthen internal visibility but also ensure evidence admissibility in legal contexts.

 doi:10.20944/preprints202510.1285.v1

For organizations, enhancing forensicability means institutionalizing proactive DFR practices—ensuring data capture, protection, and retrieval mechanisms are integral to operations. Continuous assessment through forensic readiness metrics helps organizations transition from fragile, reactive postures to resilient, evidence-supported defenses.

5.2. Evolutionary Game Theory Analysis

Using Evolutionary Game Theory (EGT) enables modeling of how attacker and defender strategies evolve concurrently over time. This approach captures adaptation cycles that traditional static game models overlook.

The simulation results in Table 9 and Figure 16 illustrate how strategy populations change across generations. Attackers and defenders adjust probabilistically based on observed payoffs, with defender readiness influencing long-term stability.

Table 9. Simulation Results Based on Evolutionary Game Theory.

Resources	Defenders	Attackers	Scenario	Final Value	Avg. Attacker Strategy	Avg. Defender Strategy	Avg. Readiness
1	10	5	a	0.56	0.84	–	0.00
1	15	5	b	0.52	0.94	–	0.00
1	25	5	c	0.61	0.69	–	0.00
3	10	5	d	0.96	0.58	–	0.00
3	25	5	f	1.00	1.00	–	0.00
5	15	5	h	0.91	0.75	–	0.03

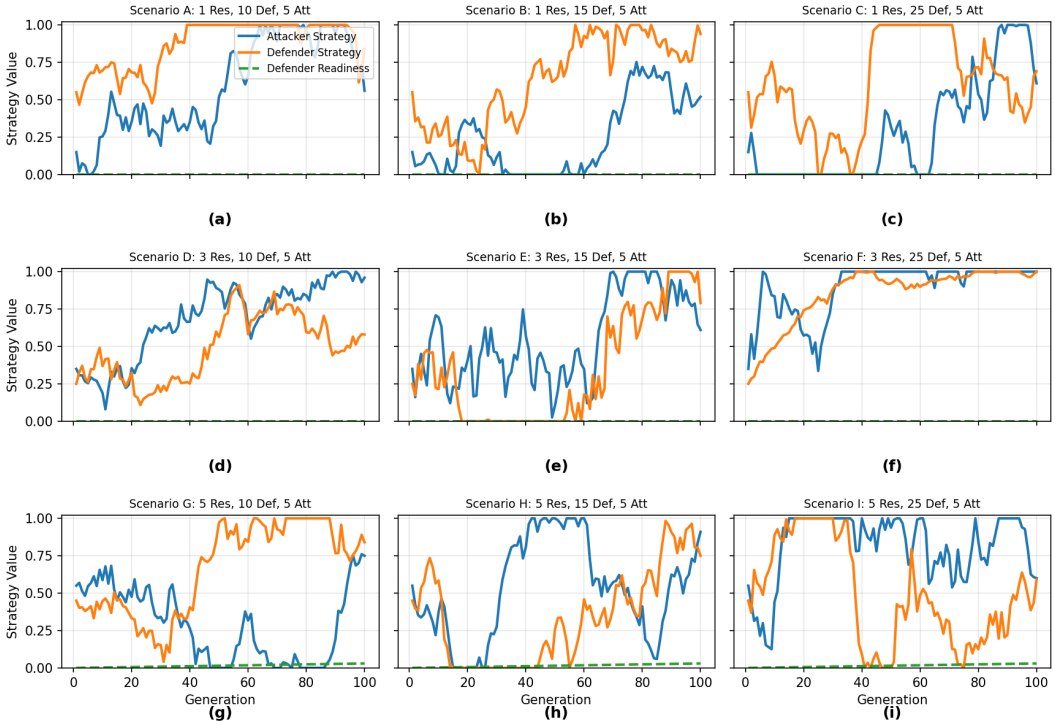


Figure 16. Evolution of attacker and defender strategies in EGT simulation.

Key insights derived from EGT include:

- **Evolutionary Dynamics:** Attackers and defenders co-adapt in continuous feedback cycles; the success of one influences the next strategic shift in the other.
- **Replication and Mutation:** Successful tactics replicate, while mutations introduce strategic diversity critical for both exploration and adaptation.
- **Equilibrium and Stability:** Evolutionary Stable Strategies (ESS) represent steady states where neither party benefits from deviation.

 doi:10.20944/preprints202510.1285.v1

- **Co-evolutionary Context:** The model exposes the perpetual nature of cyber escalation, showing that proactive defense and continuous readiness optimization are essential to remain resilient.

5.3. Attack Impact on Readiness and Investigation Phases

The simulation represented in Figure 17 demonstrates how attacks influence DFR through overlapping utility functions between attackers and defenders during investigation phases. Each incident reveals opportunities for defenders to improve readiness, forming a feedback mechanism between preparedness and investigative learning.

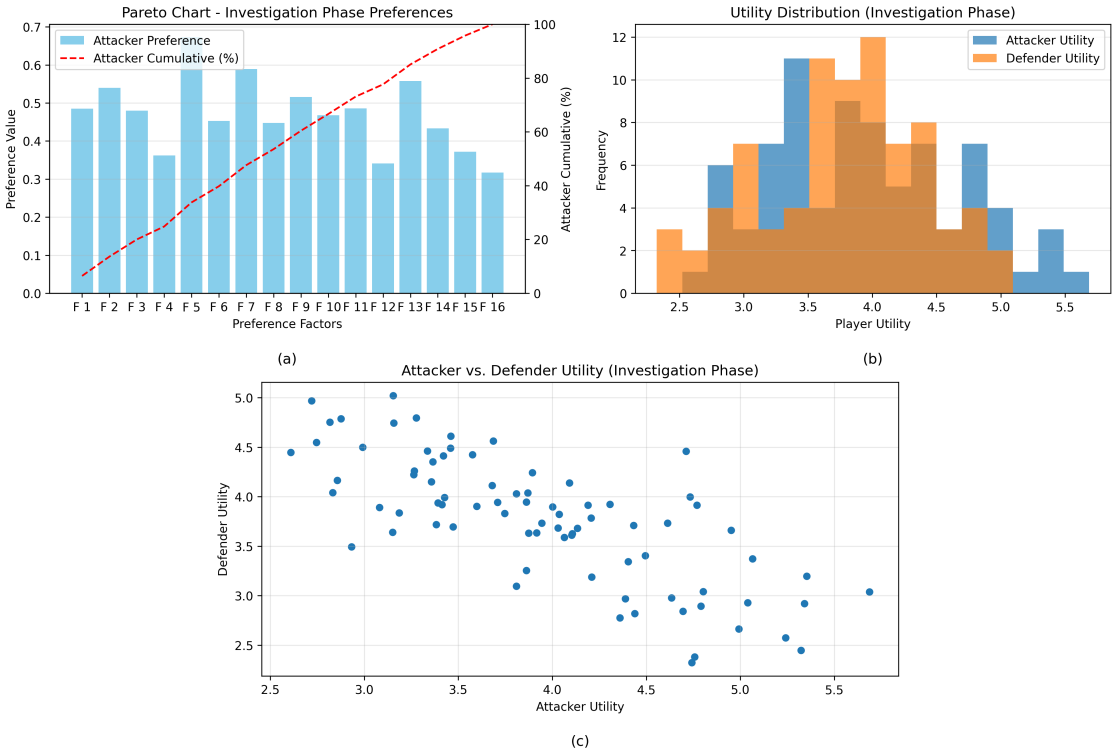


Figure 17. Effect of attacks on investigation phases: (a) Pareto chart; (b) Attacker and defender utility; (c) Utility coordination visualization.

Observed overlaps indicate that investigation phases contribute directly to capability growth—highlighting that post-incident analysis enriches strategic defense planning and improves future preparedness.

5.4. Readiness and Training Level of the Defender

Simulations comparing varying defender experience levels (Junior, Mid-level, Senior) reveal a direct correlation between training maturity and overall forensic readiness (Figure 18). Higher training levels correlate with improved detection accuracy and evidence capture, illustrating that defensive effectiveness is both strategic and skill-dependent.

 doi:10.20944/preprints202510.1285.v1

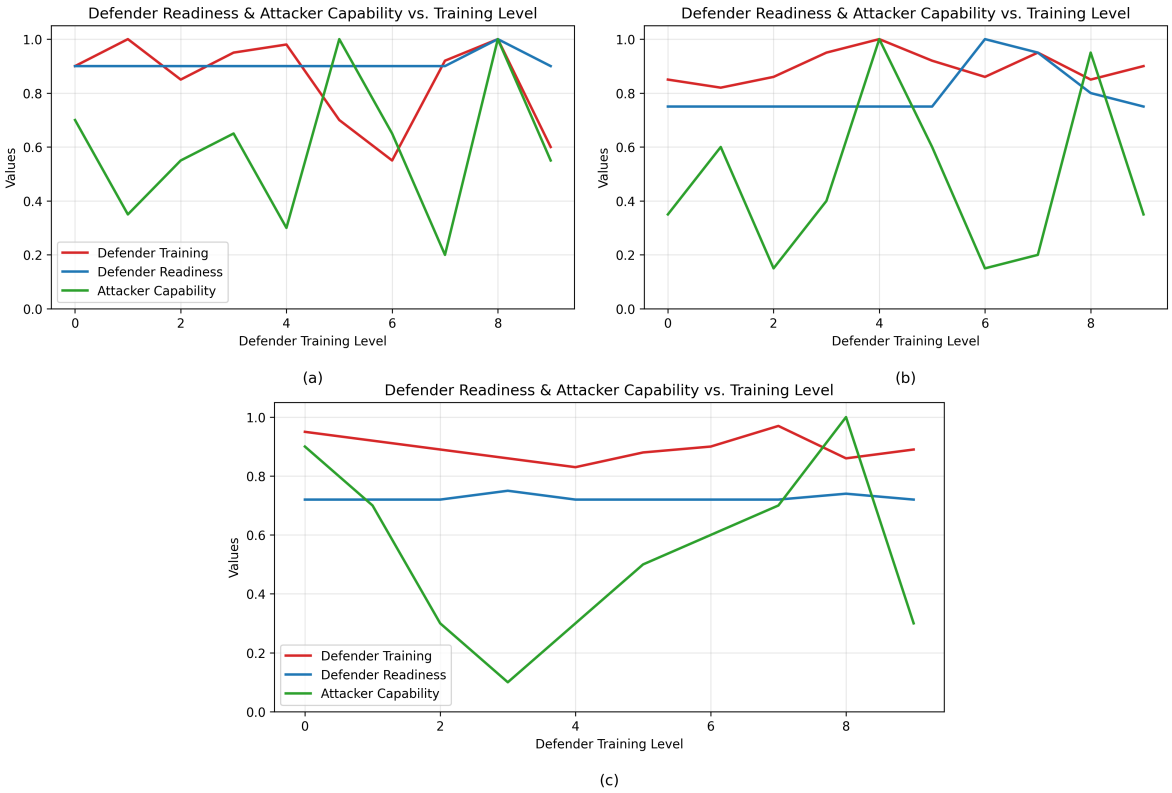


Figure 18. Defender readiness vs. training level in three maturity regimes: (a) Junior+Mid+Senior, (b) Mid+Senior, and (c) Senior.

5.5. Attack Success and Evidence Collection Rates

Monte Carlo simulations of attack outcomes (Table 10) show that higher attacker capability increases success rates, while robust forensic processes substantially raise evidence collection probability across scenarios.

Table 10. Simulation results (mean $\pm$ 95% CI; $N = 50{,}000$ trials per setting).

	Low	Medium	High
Attack success rate	0.25 ± 0.0038	0.53 ± 0.0044	0.75 ± 0.0038
Evidence collection rate	0.93 ± 0.0022	0.96 ± 0.0017	0.94 ± 0.0021

5.6. Comparative Analysis in SMB and SME Organizations

Recognizing that SMEs and SMBs differ in resource availability and defensive maturity, a comparative simulation was conducted (Tables 11–12). Results show that SMBs typically exhibit higher resilience, yet both types face elevated risks under "irrational" attacker behaviors.

Table 11. Simulation results of attack success rate for SME and SMB organizations.

ID	SME					SMB					Impact metrics			
	Type	Malic.	Str.	Impact	CVSS	Type	Malic.	Str.	Impact	CVSS	Workload	Avail.	Conf.	Integ.
0	DDoS	0.75	1.12	High	7	DDoS	0.75	1.12	High	7	1.125	0.8	0	0
1	SQLI	0.75	1.12	High	9	SQLI	0.75	1.12	High	9	2.7	2.58	7.2	7.2
2	DDoS	0.75	1.12	Med	0	DDoS	0.75	1.12	Med	0	1.125	0.96	0	0
3	SQLI	0.75	1.12	High	9	SQLI	0.75	1.12	High	9	1.125	1.005	7.2	7.2
4	DDoS	0.75	1.12	Low	0	DDoS	0.75	1.12	Low	0	1.125	0.96	0	0
5	SQLI	0.75	1.12	Med	7	SQLI	0.75	1.12	Med	7	2.7	2.58	2.8	2.8

 doi:10.20944/preprints202510.1285.v1

Table 12. Simulation result of attack success rate—irrational behavior.

ID	SME					SMB					Impact metrics			
	Type	Malic.	Str.	Impact	CVSS	Type	Malic.	Str.	Impact	CVSS	Workload	Avail.	Conf.	Integ.
0	SQLI	0.49	0.73	Med	7	SQLI	0.49	0.73	Med	7	0.73	0.61	2.8	2.8
1	DDoS	0.75	1.12	High	7	DDoS	0.75	1.12	High	7	1.12	0.80	0	0
2	DDoS	0.80	1.21	High	7	DDoS	0.80	1.21	High	7	1.21	0.80	0	0
3	SQLI	0.16	0.24	High	9	SQLI	0.16	0.24	High	9	0.24	0.12	7.2	7.2
4	SQLI	0.58	0.87	High	9	SQLI	0.58	0.87	High	9	2.45	2.33	7.2	7.2
5	DDoS	0.84	1.26	High	7	DDoS	0.84	1.26	High	7	2.84	0.80	0	0

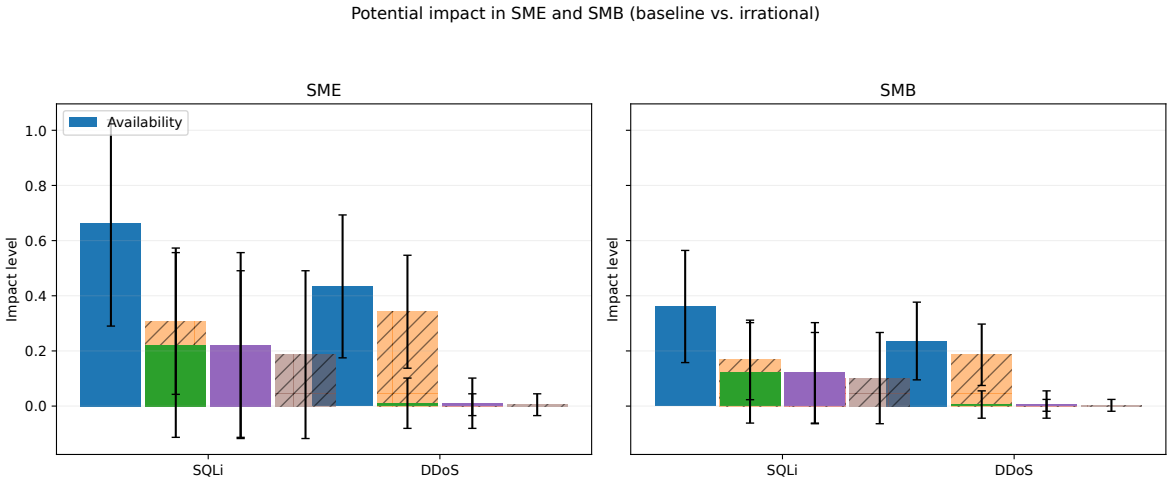


Figure 19. Impact comparison for SMEs and SMBs under SQLi and DDoS scenarios (baseline vs. irrational).

5.6.1. Irrational Attacker Behavior Analysis

By modeling partial randomness in adversarial decision-making, "irrational behavior" introduces deviations from expected attacks, thus reflecting real-world unpredictability. Figures 20 and 21 illustrate the expanded range of outcomes.

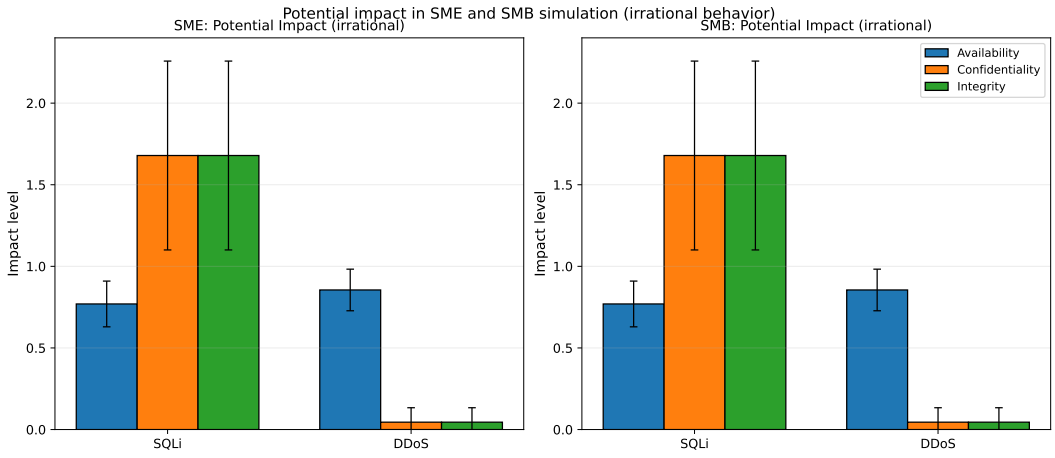


Figure 20. Impact of irrational attacker behavior on SQLi and DDoS for SME and SMB simulations.

 doi:10.20944/preprints202510.1285.v1

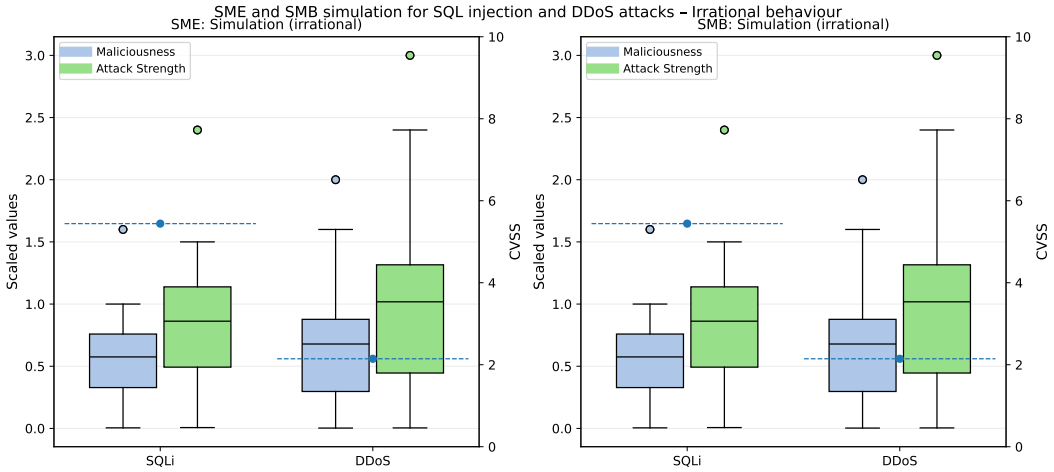


Figure 21. Behavioral distribution under irrational attack scenarios for SMEs and SMBs.

This model highlights the necessity for robust intrusion detection, endpoint monitoring, and anomaly-based analytics to counteract unpredictable threats and enhance resilience in both small- and mid-scale organizations.

5.7. Limitations and Future Work

While this research offers a structured quantitative contribution to DFR and security strategy development, certain limitations acknowledge the boundaries of current modeling:

- **Model Complexity:** Real-world human elements and deep organizational dynamics may extend beyond current model parameters.
- **Data Availability:** Reliance on open-source ATT&CK and D3FEND datasets limits coverage of emerging threat behaviors.
- **Computational Needs:** Evolutionary modeling and large-scale simulations require high-performance computing resources.
- **Expert Bias:** AHP-based weighting depends on expert judgment, introducing potential subjective bias despite structured controls.

Future research could pursue:

- **Real-time Adaptive Models:** Integrating continuous learning to instantly adapt to threat changes.
- **AI/ML Integration:** Employing predictive modeling for attacker intent recognition and defense automation.
- **Cross-Organizational Collaboration:** Expanding to cooperative game structures for shared threat response.
- **Empirical Validation:** Conducting large-scale quantitative studies to reinforce and generalize model applicability.

6. Conclusion

This study presents a comprehensive game-theoretic framework that formalizes classical strategic principles, notably those of Sun Tzu, into a structured model applicable to contemporary cyber conflict analysis. By modeling the strategic interplay between attackers and defenders, the framework bridges traditional strategic insight and modern decision-theoretic planning. It integrates MITRE ATT&CK–D3FEND mappings, incorporates readiness scoring across simulated organizational scenarios, and aligns these insights with quantitative game-theoretical analyses.

Our results identify one PNE and five MNEs. The PNE emphasizes the defender's *Detect* strategy as a robust counter to attackers' *Impact*-focused operations. MNE findings further suggest that defenders should allocate approximately 90–95% of their forensic effort toward modeling controls, preserving

 doi:10.20944/preprints202510.1285.v1

a smaller fraction for real-time detection. This balance introduces useful strategic unpredictability, increases the attacker's required effort, and diminishes overall intrusion success probabilities.

Operationally, these insights were translated into a four-phase assessment process encompassing readiness scoring, maturity classification, gap identification, and roadmap prioritization. Through this practical translation, our model enables measurable digital forensic improvements. Empirical evaluation revealed that SMEs face attacker success rates 15˜25 percentage points higher than those of SMBs under similar threat conditions. This gap largely reflects foundational deficiencies—such as inadequate logging, inconsistent volatile-data retention, and weak evidence-integrity controls. When SMEs strategically invested in high-impact defensive measures, including enhanced logging and forensic data preservation, average attacker success rates decreased by up to 30%, demonstrating the tangible value of equilibrium-based allocation.

6.1. Limitations

The framework's accuracy depends on the quality and granularity of metric data as well as expert input for AHP weighting. Factors such as organizational diversity, resource variability, and evolving adversary behaviors could influence transferability. Additionally, the assumption of static utility parameters between iterations simplifies real-world dynamics, which are inherently fluid and adaptive.

6.2. Future Research Directions

Building upon this foundation, several research extensions are envisaged:

- **Extended Environmental Applications:** Adapting the framework to cloud-native, IoT, and blockchain ecosystems where architectural differences create distinct forensic challenges.
- **Dynamic Threat Intelligence Integration:** Employing real-time data feeds and AI-based analytics to enable adaptive recalibration of utilities and strategy distributions.
- **Standardized Readiness Benchmarks:** Developing comparative industry baselines for forensic maturity that support cross-organizational evaluation and improvement.
- **Automated Response Coupling:** Integrating automated incident response and orchestration tools to bridge the gap between detection and remediation.
- **Enhanced Evolutionary Models:** Expanding evolutionary game formulations to capture longer-term strategic co-adaptations between attackers and defenders.
- **Large-Scale Empirical Validation:** Conducting multi-sector, empirical measurement campaigns to statistically validate and refine equilibrium predictions.

In conclusion, the proposed game-theoretic approach provides a mathematically grounded, strategically informed basis for advancing DFR. By linking equilibrium analysis with empirical readiness metrics, the framework offers a repeatable methodology for optimizing resource allocation, reducing attacker advantage, and fostering systemic resilience against persistent and adaptive cyber threats.

Supplementary Materials: The following supporting information can be downloaded at the website of this paper posted on Preprints.org.

Author Contributions: Conceptualization, M.V., S.J. and H.N.; methodology, M.V. and H.N.; software, M.V.; validation, M.V., S.J. and H.N.; formal analysis, M.V. and H.N.; investigation, M.V.; resources, S.J.; data curation, M.V.; writing—original draft preparation, M.V.; writing—review and editing, S.J. and H.N.; visualization, M.V.; supervision, S.J. and H.N.; project administration, S.J.; funding acquisition, not applicable. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The APC was funded by the authors.

Institutional Review Board Statement: Not applicable. The study did not involve humans or animals and therefore did not require Institutional Review Board approval.

Informed Consent Statement: Not applicable. The study did not involve humans.

 doi:10.20944/preprints202510.1285.v1

Data Availability Statement: All code and synthetic datasets supporting the findings of this study are openly available at https://github.com/Mehrn0ush/gtDFR.

Acknowledgments: This work received no external financial or in-kind support beyond the authors' personal resources.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AHP	Analytic Hierarchy Process
APT	Advanced Persistent Threat
ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
CASE	Cyber-investigation Analysis Standard Expression
CIA	Confidentiality, Integrity, Availability (triad)
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
D3FEND	MITRE Defensive Countermeasures Knowledge Graph
DFIR	Digital Forensics and Incident Response
DFR	Digital Forensic Readiness
DDoS	Distributed Denial of Service
EDR	Endpoint Detection and Response
EGT	Evolutionary Game Theory
ESS	Evolutionarily Stable Strategy
IDPS	Intrusion Detection and Prevention System
JCP	*Journal of Cybersecurity and Privacy*
MCDA	Multi-Criteria Decision Analysis
MNE	Mixed Nash Equilibrium
NDR	Network Detection and Response
NE	Nash Equilibrium
PNE	Pure Nash Equilibrium
SIEM	Security Information and Event Management
SMB	Small and Medium Business
SME	Small and Medium Enterprise
SQLi	Structured Query Language injection
TTP	Tactics, Techniques, and Procedures
UCO	Unified Cyber Ontology
XDR	Extended Detection and Response

Appendix A. Simulation Model and Settings

Readiness Components

Let $T \in [0,1]$ (training), $E \in [0,1]$ (experience), and $V \in [0,1]$ (attacker capability; larger is stronger). We define

$$C = w_T\, T + w_{\mathrm{Aw}}\, \mathrm{Aw}, \qquad F = w_E\, E + w_P\, P,$$

where Aw is security awareness and P denotes forensics procedures. We use $(w_T, w_{\mathrm{Aw}}) = (0.7, 0.3)$ and $(w_E, w_P) = (0.8, 0.2)$, with $C, F \in [0,1]$.

Outcome Probabilities

For attacker strength $s \in \{\mathrm{Low}, \mathrm{Med}, \mathrm{High}\}$,

$$p_{\mathrm{attack}}(s \mid C) = \mathrm{clip}(b_s\,[1 - \alpha\,(C - \mu_C)],\, 0,\, 1), \tag{A1}$$

$$p_{\mathrm{collect}}(s \mid F, \kappa) = \mathrm{clip}(e_s + \beta\,(F - \mu_F) - \gamma\,(\kappa - \mu_\kappa),\, 0,\, 1), \tag{A2}$$

 doi:10.20944/preprints202510.1285.v1

where $(b_{\text{Low}}, b_{\text{Med}}, b_{\text{High}}) = (0.25, 0.53, 0.75)$, $(e_{\text{Low}}, e_{\text{Med}}, e_{\text{High}}) = (0.93, 0.96, 0.94)$, $\alpha = 0.5$, $\beta = 0.20$, $\gamma = 0.25$, and $\mu_C = \mu_F = 0.75$, $\mu_\kappa = 0.60$ are centering constants. Evidence complexity $\kappa \sim \mathcal{U}(0.30, 0.90)$. The function $\text{clip}(x, 0, 1)$ truncates to $[0, 1]$.

Sampling and Maturity Regimes

For each trial we draw T, A, E, P from regime-specific ranges:

- Junior+Mid+Senior: $T \sim \mathcal{U}(0.40, 0.90)$, $E \sim \mathcal{U}(0.40, 1.00)$;
- Mid+Senior: $T \sim \mathcal{U}(0.60, 0.90)$, $E \sim \mathcal{U}(0.60, 1.00)$;
- Senior: $T \sim \mathcal{U}(0.70, 0.90)$, $E \sim \mathcal{U}(0.70, 1.00)$.

Attacker capability V used in Figure 18 is sampled per point to shape the green curve.

Experiment Size and Uncertainty

We run $N = 50{,}000$ trials per attacker strength with seed 42. Rates are reported as $\hat{p} \pm 1.96\sqrt{\hat{p}(1-\hat{p})/N}$ (95% CI).

References

1. Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In Proceedings of the Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. Springer, 2014, pp. 63–72.
2. Scott, J.S.; R.. Advanced Persistent Threats: Recognizing the Danger and Arming Your Organization. *IT Professional* **2015**, *17*.
3. Rowlingson, R. A ten step process for forensic readiness. *International Journal of Digital Evidence* **2004**, *2*, 1–28.
4. Naraine, R. Researchers spot APTs targeting small business MSPs, 2023.
5. Johnson, R. 60 percent of small companies close within 6 months of being hacked,, 2019.
6. Baker, P. The SolarWinds hack timeline: Who knew what, and when?, 2021.
7. Batool, A.; Zowghi, D.; Bano, M. AI governance: a systematic literature review. *AI and Ethics* **2025**, pp. 1–15.
8. Wrightson, T. *Advanced persistent threat hacking: the art and science of hacking any organization*; McGraw-Hill Education Group, 2014.
9. Årnes, A. *Digital forensics*; John Wiley & Sons, 2017.
10. Griffith, S.B. *Sun Tzu: The art of war*; Vol. 39, Oxford University Press London, 1963.
11. Myerson, R.B. *Game theory*; Harvard university press, 2013.
12. Belton, V.; Stewart, T. *Multiple criteria decision analysis: an integrated approach*; Springer Science & Business Media, 2002.
13. Lye, K.w.; Wing, J.M. Game strategies in network security. *International Journal of Information Security* **2005**, *4*, 71–86.
14. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences. IEEE, 2010, pp. 1–10.
15. Zhu, Q.; Basar, T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine* **2015**, *35*, 46–65.
16. Kent, K.; Chevalier, S.; Grance, T. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86* **2006**.
17. Alpcan, T.; Başar, T. Network security: A decision and game-theoretic approach. *Cambridge University Press* **2010**.
18. Casey, E. *Digital evidence and computer crime: Forensic science, computers, and the internet*; Academic press, 2011.
19. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.P. Game theory meets network security and privacy. *Acm Computing Surveys (Csur)* **2013**, *45*, 1–39.
20. Nisioti, A.; Loukas, G.; Rass, S.; Panaousis, E. Game-theoretic decision support for cyber forensic investigations. *Sensors* **2021**, *21*, 5300.
21. Hasanabadi, S.S.; Lashkari, A.H.; Ghorbani, A.A. A game-theoretic defensive approach for forensic investigators against rootkits. *Forensic Science International: Digital Investigation* **2020**, *33*, 200909.

 doi:10.20944/preprints202510.1285.v1

22. Karabiyik, U.; Karabiyik, T. A game theoretic approach for digital forensic tool selection. *Mathematics* **2020**, *8*, 774.
23. Hasanabadi, S.S.; Lashkari, A.H.; Ghorbani, A.A. A memory-based game-theoretic defensive approach for digital forensic investigators. *Forensic Science International: Digital Investigation* **2021**, *38*, 301214.
24. Caporusso, N.; Chea, S.; Abukhaled, R. A game-theoretical model of ransomware. In Proceedings of the Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9. Springer, 2018, pp. 69–78.
25. Kebande, V.R.; Venter, H.S. Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences* **2018**, *50*, 552–591.
26. Kebande, V.R.; Karie, N.M.; Choo, K.R.; Alawadi, S. Digital forensic readiness intelligence crime repository. *Security and Privacy* **2021**, *4*, e151.
27. Englbrecht, L.; Meier, S.; Pernul, G. Towards a capability maturity model for digital forensic readiness. *Wireless Networks* **2020**, *26*, 4895–4907.
28. Reddy, K.; Venter, H.S. The architecture of a digital forensic readiness management system. *Computers & security* **2013**, *32*, 73–89.
29. Grobler, C.P.; Louwrens, C. Digital forensic readiness as a component of information security best practice. In Proceedings of the IFIP International Information Security Conference. Springer, 2007, pp. 13–24.
30. Lakhdhar, Y.; Rekhis, S.; Sabir, E. A Game Theoretic Approach For Deploying Forensic Ready Systems. In Proceedings of the 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). IEEE, 2020, pp. 1–6.
31. Elyas, M.; Ahmad, A.; Maynard, S.B.; Lonie, A. Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security* **2015**, *52*, 70–89.
32. Baiquni, I.Z.; Amiruddin, A. A case study of digital forensic readiness level measurement using DiFRI model. In Proceedings of the 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2022, pp. 184–189.
33. Rawindaran, N.; Jayal, A.; Prakash, E. Cybersecurity Framework: Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5.0. *Journal of Cybersecurity and Privacy* **2025**, *5*, 17.
34. Trenwith, P.M.; Venter, H.S. Digital forensic readiness in the cloud. In Proceedings of the 2013 Information Security for South Africa. IEEE, 2013, pp. 1–5.
35. Monteiro, D.; Yu, Y.; Zisman, A.; Nuseibeh, B. Adaptive Observability for Forensic-Ready Microservice Systems. *IEEE Transactions on Services Computing* **2023**.
36. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling* **2022**, *21*, 157–177.
37. Wang, J.; Neil, M. A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples. *arXiv preprint arXiv:2106.00471* **2021**.
38. Usman, N.; Usman, S.; Khan, F.; Jan, M.A.; Sajid, A.; Alazab, M.; Watters, P. Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. *Future Generation Computer Systems* **2021**, *118*, 124–141.
39. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems* **2021**, *115*, 406–420.
40. Soltani, S.; Seno, S.A.H. Detecting the software usage on a compromised system: A triage solution for digital forensics. *Forensic Science International: Digital Investigation* **2023**, *44*, 301484.
41. Rother, C.; Chen, B. Reversing File Access Control Using Disk Forensics on Low-Level Flash Memory. *Journal of Cybersecurity and Privacy* **2024**, *4*, 805–822.
42. Nikkel, B. Registration Data Access Protocol (RDAP) for digital forensic investigators. *Digital Investigation* **2017**, *22*, 133–141.
43. Nikkel, B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation* **2020**, *33*, 200908.
44. Seo, S.; Seok, B.; Lee, C. Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing* **2023**, *79*, 9467–9485.
45. Malhotra, S. Digital forensics meets ai: A game-changer for the 4th industrial revolution. In *Artificial Intelligence and Blockchain in Digital Forensics*; River Publishers, 2023; pp. 1–20.
46. Tok, Y.C.; Chattopadhyay, S. Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation* **2023**, *45*, 301540.

 doi:10.20944/preprints202510.1285.v1

47. Han, K.; Choi, J.H.; Choi, Y.; Lee, G.M.; Whinston, A.B. Security defense against long-term and stealthy cyberattacks. *Decision Support Systems* **2023**, *166*, 113912.
48. Chandra, A.; Snowe, M.J. A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems* **2020**, *38*, 100467.
49. Casey, E.; Barnum, S.; Griffith, R.; Snyder, J.; van Beek, H.; Nelson, A. Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. *Digital investigation* **2017**, *22*, 14–45.
50. Dyer, M.E. The complexity of vertex enumeration methods. *Mathematics of Operations Research* **1983**, *8*, 381–402.
51. Knight, V.; Campbell, J. Nashpy: A Python library for the computation of Nash equilibria. *Journal of Open Source Software* **2018**, *3*, 904.
52. Zopounidis, C.; Pardalos, P.M. *Handbook of multicriteria analysis*; Vol. 103, Springer Science & Business Media, 2010.
53. Bipm, I.; Ifcc, I.; Iso, I. IUPaP, and OImL. *Evaluation of measurement data—Supplement* **2008**, *1*.
54. Saaty, T.L. Analytic hierarchy process. In *Encyclopedia of operations research and management science*; Springer, 2013; pp. 52–64.