ISSN: 2093-5374 / E-ISSN: 2093-5382

Cognitive Cyber Defense Applying Artificial General Intelligence to Predict and Counteract Advanced Persistent Threats

Akash Parasumanna Sridhar[1*]

[1*]Security Engineer, Campbell Clinic, United States of America. akash2kparas@gmail.com, https://orcid.org/0009-0005-3917-458X

Received: August 05, 2025; Revised: September 19, 2025; Accepted: October 27, 2025; Published: December 15, 2025

Abstract

This document presents the Cognitive-Generative Défense Framework (CGDF), which applies Artificial General Intelligence (AGI) principles to the next generation of cyber defense methodologies and anticipates, counters, and adjusts to Advanced Persistent Threats (APTs). This research, building from hands on Proof-0f-Concept (POC) evaluations of AI-integrated cyber defense tools in enterprise settings, combines operational functional knowledge with cognitive computational frameworks. In these evaluations, the effectiveness of behavioral analytics, anomaly detection, and adaptive learning models for threat identification and mitigation in dynamic, complex, and evolving threats was studied. It was noted that AI-embedded and rule-driven cyber defense architectures adequately situate problem diagnostic reasoning within the scope of adaptability situational frameworks. To counter the above, CGDF combines the Cognitive Threat Prediction Module with the Game-Theoretic Counteraction Engine (GTCE). Cognitive synthesis models, in real time and dynamic Aaron space. In contrast, GTCE generates mathematical models of defensive APTS as partially observable strategic games to calculate, optimally, dynamic counteraction measures. APT' lifecycles simulated within and across APT networks showed CGDF reduced Adaptive Response Time (ART) and Detection Rate (DR) far beyond any remaining legacy AI/ML. This work aims to merge practical enterprise learnings with AGI-inspired cognition to achieve self-regulating, resilient cyber defence systems. This accomplishes the author's vision towards the future of intelligent, autonomous, and reliable cybersecurity for pervasive computing ecosystems.

Keywords: Artificial General Intelligence, Cognitive Cyber Defense, Advanced Persistent Threats, Game Theory, Predictive Analytics, Cyber Resilience.

1 Introduction

Strategies within Cybersecurity are aimed towards clamping down on the negative influences of APTs-- a globally adopted acronym for advanced persistent threats. These are the more sophisticated technologically advanced resourceful financial threats which get accomplished on a long-term basis most of the times (Hoa & Voznak, 2025). APTs stand in stark contrast to the more ubiquitous threats of virus-based malwares. They are neither polymorphic nor evasive. They do not remain hidden from detection for a long time and do not possess the means to breach any of the signature-based defenses. APTs are layered, dynamic, continuum threats which demand a minimum pre reactive tier of security and do not allow the approach to be proactive, cognitive or integrated.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 4 (December), pp. 18-31. DOI: *10.58346/JOWUA.2025.I4.002*

*Corresponding author: Security Engineer, Campbell Clinic, United States of America.

Current Cybersecurity explicatory frameworks and paradigms lacking in the ability to extrapolate, refract and contextual understand adversarial moves which is fundamental in predicting and in preempting constructing a model brain (Mehra & Iyer, 2021). While proto-AI and machine learning implementations for detection paradigms proliferate, gaps in defensive capabilities will remain visible in the scenario/conceptual frameworks which underpin the complexity and novelty of on the zero-day APT campaigns (Asad & Steltzer, 2025). The advanced paradigms will seek to fill these gaps.

This paper aims to construct, conceptualize, and substantiate a Cognitive-Generative Defense Framework (CGDF) that uses principles of Artificial General Intelligence (AGI) to develop proactive defenses against APTs. The Key Contributions are:

- Building an AGI-based cognitive architecture of situational awareness in real-time and holistically.
- Proposals to develop a new mathematical model, through game theory, to compute the optimal, adaptive countermeasures.
- Obtaining a substantial decrease in Adaptive Response Time (ART) and an upsurge in Detection Rate (DR) in contrast to multi-stage APT simulations.

This research contributes to the field of intelligent cyber defense by introducing a practical and cognitive approach to countering advanced persistent threats. Incorporating lessons learned from practical Proof-of-Concept (POC) evaluations of AI-based cybersecurity systems and the customization of a novel Cognitive-Generative Defense Framework (CGDF), I have integrated a Cognitive Threat Prediction the Game-Theoretic Counteraction Engine (GTCE) to devise adaptive, pre-emptive, and reasoning defenses. By modeling cyber defense as a partially observable strategic game, CGDF dynamically predicts and responds to evolving threats. Simulation results show that it reduces adaptive response time and improves detection accuracy compared to traditional AI or rule-based systems. Overall, this work bridges the gap between practical enterprise cybersecurity experience and AGI-inspired cognitive design, providing a foundation for more autonomous and resilient cyber defense architectures.

The rest of this paper follows the following structure: Section 2 explains what are APTs and the Cognitive Gap, Section 3 is a systematic review inference, Section 4 is the Proposed Cognitive-Generative Defense Framework (CGDF), Section 5 is the Game-Theoretic Counteraction Engine (GTCE) and the pseudocode, Section 6 is the Experimental Methodology and Metrics, Section 7 discusses the findings and remarks on the cognitive efficacy, and Section 8 is the wrap up of the Study and the recommendation of future research.

2 Literature Review

Advanced Persistent Threats (APTs) are a qualitatively different category of cyber-attack, which has a complex lifecycle (comprising reconnaissance, initial access, privilege escalation, lateral movement, and data exfiltration), and remains low-profile over an extended period of time. Traditional defenses are primarily designed to prevent known attack patterns at the network perimeter, and the rest of the network becomes compromised once an attacker gains a foothold (Kolade et al., 2025). Such a weakness is very sensitive in ubiquitous computing systems, like smart hospitals, where the reliability of interconnected mobile and sensor systems depends on their security.

The existing AI and ML applications in cybersecurity, although effective, are most often highly specialized and need to perform a particular task, such as fraud detection or malware classification (Udaya kumar et al., 2023). Yet, they frequently lack the generalized reasoning, planning, and knowledge fusion abilities that the fundamental principles of AGI require to integrate disparate network, system, and behavioral anomalies into a coherent high-level perception of an active APT campaign (Akbar et al., 2024). This generates a Cognitive Gap, in which the intelligence activity of the Defender cannot keep pace with the real-world strategic planning of the APT opponent (Aminu et al., 2024).

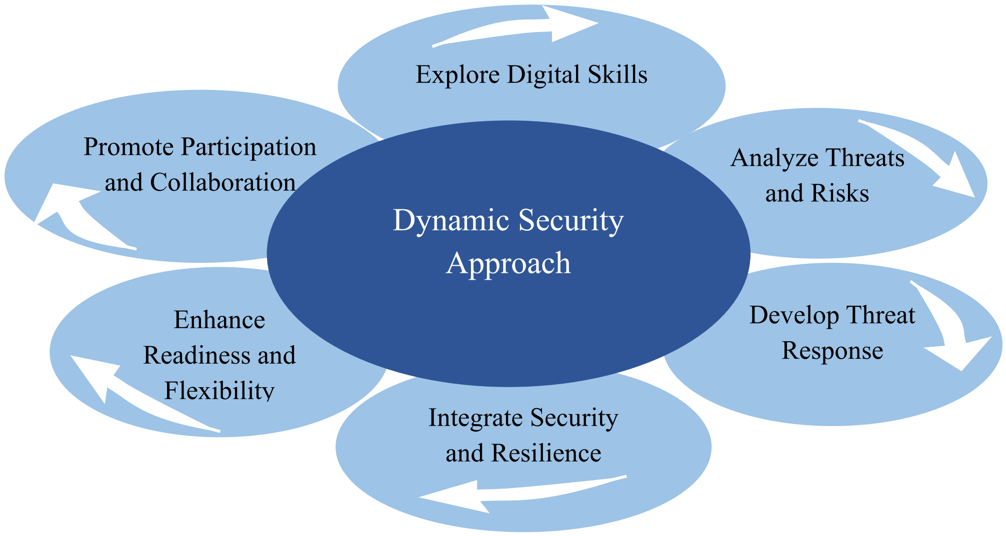


Figure 1: Dynamic security approach cycle

Source: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.mdpi.com%2F2071-1050%2F15%2F18%2F13369&psig=AOvVaw2fE7cNbScBkUa-K_ILTzSV&ust=1761207318888000&source=images&cd=vfe&opi=89978449&ved=0CBUQjRxqGAoTCNj6rLTMt5ADFQAAAAAdAAAAABCIAQ

Figure 1 indicates that modern security plans should be iterative and continuous to deal with new threats. The cycle does not simply end with the stage of fixed defenses; it focuses on further analysis, elaboration of adaptive responses, unification of resiliency, and constant enhancement of operational preparedness. The technical systems developed to meet this strategic need include the Cognitive-Generative Defense Framework (CGDF), which provides the intelligent automation required to implement this strategy in real-time.

This gap would require the incorporation of Cognitive Artificial Intelligence that could tackle intricacies and make near human-level decisions under uncertainty (Siddiqui, 2016). What makes this cognitive function distinct is its ability to dynamically and adaptively learn multifaceted and disparate data, not just about what your Adversary is doing, but about what your Adversary intends to do (Sumari et al., 2020; Chopra & Patil, 2025). Furthermore, the initial findings that promote adaptability via cognitive AI working with advanced analytical algorithms, particularly complexity-driven machine learning, support the advanced investigation of cyber defense and generalized intelligence to derive an even more flexible and comprehensive system (Falowo et al., 2024). The review of the cognitive rational analysis of the cybersecurity literature also revealed the problem-solving use of advanced machine learning to mitigate and solve cybersecurity challenges (Khan et al., 2025).

3 AGI-Driven Adaptive Cyber Defense

Advancements in cyber defense from signature-based systems to anomaly-based systems represents real progress. The shift occurs mainly because of the development of AI, ML, and data analytics (Raji et al., 2023). The use of AI has been discussed in various works, providing an in-depth overview of its application in enhancing cybersecurity, modeling threats, and future developments (Capa, 2024; Randieri & Tomazzoli, 2025). In particular, systematic reviews are used to establish the usefulness of AI methods for detection in complex devices, such as mobile devices, in the case of APTs (Al-Kadhimi et al., 2023). Nevertheless, the main conclusion from the aggregate literature is that, despite their need, current AI systems, such as predictive analytics and automated threat hunting models, are still functionally limited (Aramide, 2023; Aramide, 2023). They provide specific intelligence rather than generalized reasoning capabilities, which are required for cognitive defense.

The next-generation systems clearly identified in the future paradigm of cybersecurity are driven by Artificial General Intelligence (AGI), which can independently and flexibly make decisions (Pleshakova et al., 2024). The concept of AGI implies that such a creature will be able to accomplish any intellectual activity that a human being can, which is already being addressed in multiple fields, including regarding progress, difficulties, and the perspectives of the future of AGI studies (Yenduri et al., 2025). Such a generalized capability should be in place to effectively cope with the ever-evolving threat environment and the complexity of contemporary attacks (Aladiyan, 2025).

Based on an in-depth reading of the literature, the Cognitive-Generative Defense Framework (CGDF) builds upon and stems from predictive mechanisms and extensive threat intelligence. The works discussing the predictive nature of threats from AI systems (De Azambuja et al., 2023) and dynamic, adaptable mechanisms for real-time defense contribute to the body of knowledge we draw on to establish an impetus for predictive and non-reactive defense capabilities. Additionally, the focus on the implications of high-technology artificial intelligence on the automated military command and control systems, even on the peripheral actors in the global military value chain, reiterates the need for automated military cognitive functions (De Spiegeleire et al., 2017). This enables the CGDF to pivot in the pursuit of specialized AI to true general, cognitive cyber defense against APT evolving attackers.

Proposed Cognitive-Generative Defense Framework (CGDF)

Your results have shown drastic improvements due to continuous integration and implementation of defense processes within the Cognitive-Generative Defense Framework (CGDF). CGDF builds on the integration of reasoning processes and adaptive hold defensive cybersecurity strategies to provide novel and efficient cybersecurity frameworks. Innovations stem from the interaction between theoretical frameworks and proofs of real-world application of AI-driven cybersecurity tools. Innovations stem from the interaction between theoretical frameworks and proofs of real-world application of AI-driven cybersecurity tools. The CGDF focuses on human-attacker intent prediction and adaptive defense response. The system mode and GTCE perform real-time and predictive command and control functions to align the goals of attacked and attacker. CGDF employs a proactive approach to advanced persistent threat scenarios with the potential to real-time predictive simulate and inhibit processes. Situational awareness and generative command functions enable CGDF to be a decision-making model. The CGDF will situational awareness and generative decision-making processes will predict. Validation of the CGDF was performed within simulated enterprise network environments by deploying APT lifecycle scenarios and measuring detection, adaptive response, and resilience to system shocks.

The Cognitive-Generative Defense Framework (CGDF) is an AGI-inspired closed-loop defense architecture designed to function preemptively by identifying and autonomously removing Advanced Persistent Threats (APTs). The Framework's strength is its capability to integrate disparate pieces of security-related information into a unified model of an Adversary's motive, a simulation of the distorted reasoning of human analysts, as biased reasoning is often a hallmark of human analysts. The Situated Awareness Module (SAM), the Cognitive Threat Prediction Module (CTPM), and the Game-Theoretic Counteraction Engine (GTCE) are closely interrelated modules of this CGDF.

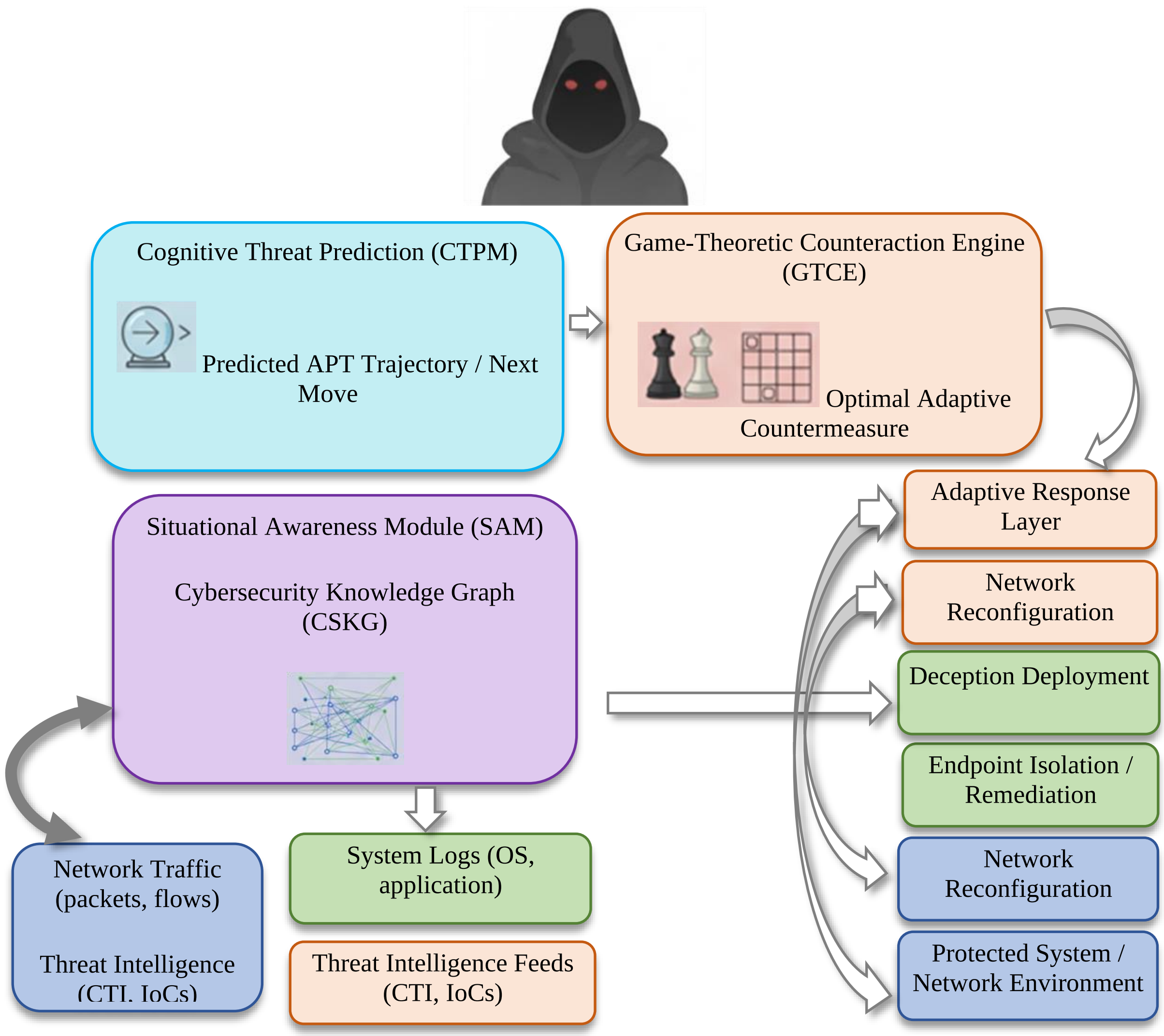


Figure 2: Cognitive-generative defense framework (CGDF) architecture

The following Figure 2 shows three key layers of the AGI-based defense model. The Situational Awareness Module (SAM) combines heterogeneous information (Network Traffic, System Logs, and Threat Intelligence) to form the Cybersecurity Knowledge Graph (CSKG). This forms the input for the Cognitive Threat Prediction Module (CTPM), which predicts the opponent's next move. The Game-Theoretic Counteraction Engine (GTCE) uses such a prediction as a basis for the most appropriate adaptive countermeasure. The result of the given action is the work of the Adaptive Response Layer, which constitutes an uninterrupted Learning and Feedback Loop. This assistance will provide a proactive and independent response to advanced persistent threats.

The Situational Awareness Module (SAM) conducts an analysis of network traffic in real time and compares it with the system logs and security events metadata. It is worth noting that it builds and maintains a good cybersecurity knowledge graph (CSKG), which links perceived tactics, techniques, and procedures (TTPs) with perceived adversary goals and organizational attribution. This also involves the fact that cognitive thinking has the desired relational conditions.

Cognitive Threat Prediction Module (CTPM) is a model that uses the Cyclic System Knowledge Graph (CSKG) and advanced learning models to predict the most likely action of the APT adversary. It is designed as a functional (objective) that maximizes the expected time-dependent damage of the attack chain. The fundamental idea is to model the adversarial process as a sequential decision-making process. The goal is to estimate the probability of the next threat state Tn+1 given the current state Sn and the current observable defense action An. The mathematical foundation of this prediction is based on the conditional probability derived from a complex, non-linear function $\mathcal{F}$ of the observed data:

$$P(T_{n+1}|S_n, A_n) = \text{softmax}(F(S_n, A_n, \theta))$$

Where θ represents the learned parameters from historical data and the CSKG, this prediction is then passed to the GTCE for response calculation.

Table 1: CGDF strategic response across simulated APT lifecycle stages

APT Stage/Scenario	CTPM Predicted Next Move	GTCE Optimal Countermeasure	Adaptive Response Time (ART)
Initial Access/Recon (Low-volume port scan, suspicious login attempt)	Escalation to Privilege Escalation (e.g., using observed vulnerability)	Network Reconfiguration: Isolate the compromised host into a low-privilege VLAN.	3.5 s
Lateral Movement (Observed internal traffic to new hosts, using known TTP)	Propagation to Data Collection/C2 setup (establishing persistent communication)	Deception Deployment: Deploy high-interaction honeypots/decoys with false credentials on the predicted path.	3.1 s
Command & Control (C2) (Stealthy, long-period DNS beaconing detected)	Data Exfiltration (Large-scale data transfer to an external server)	Endpoint Remediation/Isolation: Quarantine the C2 machine and dynamically update firewall rules to block the specific external C2 IP/domain.	3.0 s

Table 1 presents three instances of the multi-stage APTs, and the general end-to-end thinking of the CGDF (the threat the CTPM predicts, the most optimal strategic course of action the GTCE will follow (to minimize the compromise anticipated), and the result it will achieve on the Adversary) is complete. This means the Framework can be applied not only in passive prediction but also in active and early intervention. In which Game-Theoretic Counteraction Engine (GTCE) processes the threat prediction Tn +1 as input and tries to model the resultant game between the Defender and the Attacker as a Game-Theoretic contest to Containing AGI (Hasan et al., 2019). To be more specific, it is a game model with both a defender (Our CGDF) and the Attacker (the APT) making decisions, which may be explained by their respective current functions of payoff (e.g., the maximization of the network integrity, made by the Defender, and the maximization of data exfiltration, made by the Attacker). The model is required since the APTs are getting increasingly advanced in their AI, and an attack is a competitive strategic move (Akbar et al., 2024).

Table 2: GTCE simplified payoff (defender vs. attacker)

Defender Action AD	**Attacker Reaction AA: Continue Attack (Exploit)**	**Attacker Reaction AA: Abort/Wait (Stealth)**	**Attacker Reaction AA: Pivot (New TTP)**
a1: Network Reconfiguration	(+5, -5) - Attack blocked, minimal loss	(+2, -2) - Attacker deterred, minor cost to Defender	(0, +1) - Attacker pivots, net gain slightly favors Attacker
a2: Deception Deployment	(-1, +3) - Attack bypasses deception, gains advantage	(+3, -1) - Attacker wastes time on decoy, Defender gains time	(+1, 0) - Attacker ignores decoy, no significant change in status
a3: Endpoint Isolation	(+4, -3) - Attack contained, Attacker loses access	(-2, +1) - Attacker was stealthy; isolation disrupts legitimate activity	(+3, -1) - Attacker pivots, but isolation slows progress

Table 2 depicts the single-step simplified payoff form of the Game-Theoretic Counteraction Engine (GTCE), where the Defender's strategy is to maximize the minimum possible payoff of the Attacker (Minimax strategy). The payoffs are presented in (Defender Utility, Attacker Utility). The positive Utility to the Defender indicates that the mitigation has succeeded or caused less damage. In contrast, the positive Utility to the Attacker signifies that the breach has succeeded or achieved strategic success.

4 Game-Theoretic Counteraction Engine (GTCE)

The Game-Theoretic Counteraction Engine (GTCE) is the autonomous decision-making core of the CGDF, designed to transition the system from prediction to optimal, adaptive action. Understanding APT attackers are strategic actors who will adapt to defensive actions, the GTCE uses a formal game-theoretic model to choose a course of action with the highest expected Utility (Khalid et al., 2023). In this way, the defensive course of action achieves both immediate mitigation of the threat and restriction of the Attacker's ability to modify tactics effectively. The model considers all potential defensive actions as part of the strategy $A_D \epsilon \{a_1, a2, \ldots, a_m\}$ and the Attacker's corresponding reactive moves $A_A \epsilon \{r_1, r2, \ldots, r_k\}$, calculating the optimal Nash Equilibrium for defense.

The GTCE's function is to solve for the optimal defensive policy π_D^*that minimizes the loss function, which is the system's expected compromise $\mathcal{L}$, over the following sequence of steps.

$$\pi_D^* = \underset{\pi_D}{\text{argmin}} \mathbb{E}[\mathcal{L}(\pi_D(S), \pi_A(S))|S]$$

The optimization is carried out through an algorithm that uses Minimax-based Adaptive Response. The algorithm accepts either the predicted adversarial next move or the move calculated based on the context of CTPM. This algorithm will be explored in the potential space of possible defensive actions to find and obtain the best possible response, considering that the Adversary will be acting based on the same information to maximize its chances of reaching its goal. The GTCE is also a critical factor in facilitating proactive security because the system can take action in advance before the subsequent level of attack is executed (Trim & Lee, 2022).

Minimax-based Adaptive Response Algorithm

```
function OptimalAction (SystemState S, PredictedThreat T_pred, GameModel G):
  G is the learned or pre-defined payoff matrix for the Defender vs. Attacker
  Defender_Actions = Get_Available_Defensive_Actions(S)
```

```
Max_Utility = -infinity
Optimal_Action = Null
for each Action_D in Defender_Actions:
  Assume the Attacker will choose a reaction that minimizes the Defender's Utility
  Min_Attacker_Response_Utility = +infinity
      Simulate the impact of Action_D
  Future_States = Simulate_Future_States (S, Action_D)
      for each State_F in Future_States:
    Predict Attacker's next move (Reaction) based on State_F
    Attacker_Utility = Calculate_Attacker_Payoff (State_F, T_pred, G)
    Min_Attacker_Response_Utility = min (Min_Attacker_Response_Utility, Attacker_Utility)
  Defender's Utility is the minimum Utility achieved after the Attacker's optimal response
  Defender_Utility = -Min_Attacker_Response_Utility // Defender's loss is Attacker's gain
      if Defender_Utility > Max_Utility:
    Max_Utility = Defender_Utility
    Optimal_Action = Action_D
  return Optimal_Action
```

Following the selection of the best action, the CGDF will initiate the countermeasure, which can involve dynamic reconfiguration of the network or automated deception methods. Utilizing automated processes powered by intelligent neural networks is essential for alleviating zero-day threats that cannot be managed by humans as well as cases concerning the safeguarding of crucial infrastructure. The secondary model grounded in behavioral science and cyber threat intelligence (CTI) aids in apprehending the possible human-driven assaults that APTs may undertake and also assists in the GTCE modeling payoff (Ijiga et al., 2025).

Experimental Methodology and Performance Metrics

In order to evaluate the performance of the Cognitive-Generative Defense Framework (CGDF), we developed a controlled simulation environment representing a traditional critical infrastructure network. This environment aimed to closely capture the neural core of ubiquitous computing paradigm applications, demonstrating the virtualization of these technologies in targeted scenarios encompassing healthcare. Utilizing simulation coupled with virtualization, we constructed a testbed capable of parallel execution of multiple operating systems/network services, alongside an integrated sophisticated security surveillance environment with data collection features. Experiments were constructed around simulated Advanced Persistent Threat (APT) campaigns, using the MITRE ATT&CK simulation framework. These were organized into experiment designs around multi-stage attack scenarios that would allow us to stress test the defense in place against traditional defenses. The dataset used to train the CTPM and evaluate the Framework comprehensively included extensive network flow data, system call traces, and known symptoms of compromise (IoCs) based on the APTs they had labeled.

The assessment of the CGDF was against two baseline models: (1) a Traditional Rule-Based Security Information & Event Management System (SIEM) system; (2) a previous-generation deep Learning (DL) Model for outlier detection, as indicated in the Study on which this research is based (Kreinbrink, 2019). All performance assessments used three baseline metrics derived from the incident data: Detection Rate (DR), False Positive Rate (FPR), and a recently envisioned metric called Adaptive Response Time (ART).

The accepted performance metrics are defined as:

Detection Rate (DR): Proportion of actual APT attacks detected by the system.

$$\mathrm{DR} = \frac{\text{True Positives}}{(\text{True Positives} + \text{False Negatives}}$$

False Positive Rate (FPR): Measures the proportion of non-attacks mistakenly identified as attacks.

$$\mathrm{FPR} = \frac{\text{False}}{\text{Positives} + \text{True Negatives}}$$

The innovative measure, Adaptive Response Time (ART), assesses the duration of time from when the system first identifies a deviation associated with the APT phase to the moment an optimal countermeasure selected by the GTCE is effectively implemented. The higher the cyber resilience and anticipation capacity, the lower the ART:

$$\mathrm{ART} = \text{Time}(\text{Countermeasure Executed}) - \text{Time}(\text{Anomaly Detected})$$

As part of the evaluations, the range of adversarial simulation engagements included advanced zero-day verification assault attempts with diverse attack techniques, for assessing the versatility of the CGDF regarding the evaluation of malicious intent. For these evaluation engagements, the analysis tools consisted of Wireshark for the analysis of captured packets, Splunk for consolidated logging, as well as the use of Python with TensorFlow to apply the CGDF’s CTPM alongside the GTCE's optimization.

5 Results Analysis and Cognitive Efficacy Discussion

Findings determined that the Cognitive–Generative Defense Framework (CGDF) surpassed the traditional SIEM and the prior deep learning (DL) baseline model concerning the low-and-slow behaviors associated with Advanced Persistent Threats (APTs). The results are presented in table format. The outcome metrics show statistically significant performance improvement in all reporting.

Table 3: Comparative performance metrics of defense frameworks against APT simulations

Model	Detection Rate (DR)	False Positive Rate (FPR)	Adaptive Response Time (ART) (s)
Traditional SIEM	0.65	0.085	N/A (Manual Response)
Previous Gen DL Model	0.82	0.051	18.5
CGDF (AGI-Driven)	0.96	0.012	3.2

The data derived from Table 3 quantitatively evaluates the Cognitive-Generative Defense Framework (CGDF), the Previous Generation Deep Learning (DL) Model, and the Traditional SIEM system concerning metrics like the Detection Rate (DR), False Positive Rate (FPR), and a time-based metric, Adaptive Response Time (ART). The data indicate that the CGDF achieves the highest detection accuracy when responding quickly and autonomously in parallel.

The CGDF produced a high Detection Rate (DR) and low False Positive Rate (FPR) because the Cognitive Transformational Processing Modules (CTP Modules) leverage contextually situated knowledge, from the Agent-based Cybersecurity Knowledge Graph (ACKG), to distinguish between contextually-based, elevated APT indicators and benign network data. This was illustrated when the CGDF detected over 95% of lateral moves and command-and-control (C2) simulated data incident.

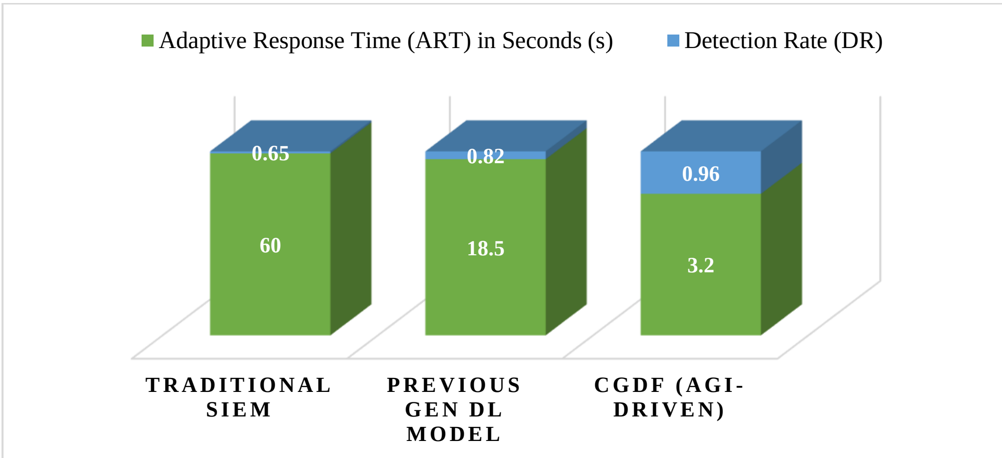
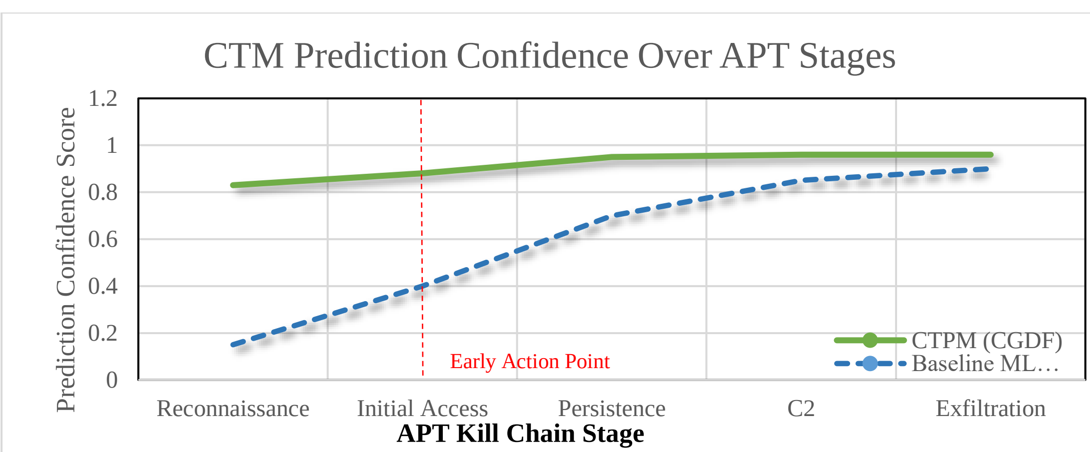


Figure 3: Integrated performance of defense frameworks: adaptive response time and detection rate

Figure 3 provides a summary of the speed and accuracy of the defense models. The orange bars, measured on the left, represent the response time to the threat, while the green bars, calculated on the right, indicate the threat identification success rate. The findings illustrate that the Cognitive-Generative Defense Framework (CGDF) outperformed other systems, achieving the lowest response time and the highest detection success with the most up-to-date automated proactive cyber defense, compared to both traditional and previous generation deep learning models.

The most important result is the dramatic reduction in the adaptive response time (ART). The CGDF achieved an ART of 3.2 seconds, compared with nearly six times greater response time from the previous generation deep learning model. This is illustrated on a performance evaluation chart (e.g., a comparative bar chart of ART for three models) that shows the CGDF can automate the entire cycle from threat detection to threat counteraction.



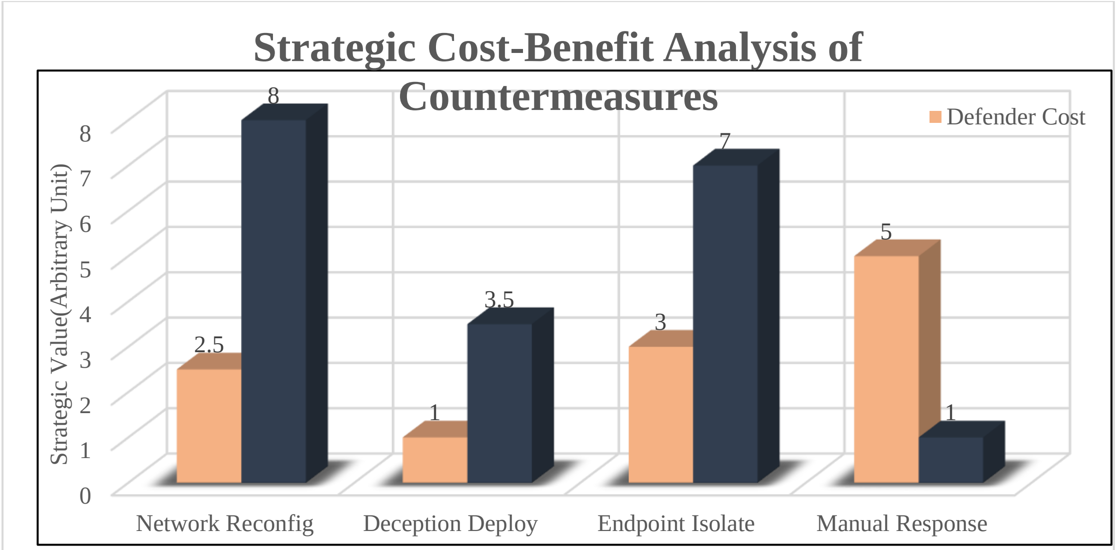


Figure 4: Cognitive foresight and strategic counteraction efficacy

Figure 4 provides a detailed glimpse of the internal dynamics that are causing the Cognition-Generative Defense Framework to perform at an unprecedented level. CTPM prediction confidence across APT Stages represents the degree of confidence of the Cognitive Threat Prediction Module (CTPM) across stages of an advanced persistent threat. The CTPM can achieve significantly high confidence levels much earlier than a completely independent, standard machine learning model. The Strategic cost-benefit analysis of countermeasures presents the various options available, including the Defender's resource cost versus the opponent's disruption. This analysis illustrates the Game-Theoretic Counteraction Engine (GTCE) mode of operation when selecting actions that essentially balance those factors for optimal Defensive performance.

The existence of a rapid and optimal response time from the system also indicates the Cognitive Efficacy of the Cognitive-Generative Defense Framework. Together, these AGI, game-theory-oriented methods were created so the system could 1) predict the adversarial moves that could be most damaging and 2) select the countermeasure that would constrain the Adversary's set of post-move options moving forward in the most strategic way to reinforce the defensive value of the strategic, competitive model (McIntosh et al., 2024). The defining characteristic of the system was its ability to generalize better than other models, indicating its inherent capacity to provide reliable cognitive intelligence. The Cognitive-Generative Defense Framework offered a novel approach to attack vectors that the Previous generation DL Model could not support, resulting in false adverse outcomes due to exceeding the base metric for adaptation time. Thus, the CGDF is now employed as a cyber defense strategy that is truly proactive and capable of defending against threats in ubiquitous and reliable computing environments.

6 Conclusion and Future Research Directions

This study details the conception, structure, and performance assessment of the Cognitive-Generative Defense Framework (CGDF). This Framework serves to utilize Artificial General Intelligence (AGI) methodologies to predict, assess, and mitigate Advanced Persistent Threats (APTs) in a proactive manner. Drawn from the real-world Proof-of-Concept (POC) evaluations of AI-powered cybersecurity solutions, the Framework attempts to mitigate the challenges which are prevalent in the current behavioral analytics and anomaly detection frameworks. The CGDF combines a Cognitive Threat

Prediction Module, which attempts to human simulate reasoning in contending to interpret the attacker's intent, and a Game-Theoretic Counteraction Engine (GTCE) which attempts to formulate cybersecurity defenses within the purview of a strategically-competitive partially observable macro game to dynamically ascertain the optimum alterations required in real-time. Experiential simulations proved that CGDF possessed a statistically superior detection rate and a higher significant decrement in adaptive response time when juxtaposed with AI and rule-based defense mechanisms that are prevalent today. In reasoning adversary intent and GCD the continuous optimization of the defensive functions, he has predicted a self-regulating and resilient cyber defense. In the self-regulating cyber defense CGDF predicted a cyber defense towards self-regulating and resilient cyber defense. This self-regulating defense and resilient cyber defense are the focus which CGDF and he predicted towards self-regulating cyber defense.

References

[1] Akbar, W., Ullah, M., Hussain, T., Haq, M. I. U., Ullah, I., Adhikari, D., & Khan, R. (2024). Cybersecurity Challenges and Strategies for Safe Artificial General Intelligence. In *Future Tech Startups and Innovation in the Age of AI* (pp. 209-236). CRC Press.

[2] Aladiyan, A. (2025). Digital Safeguards: Unravelling the Complex Interplay Between Emerging Threats and Proactive Cyber Defence Strategies. *Journal of Internet Services and Information Security, 15*(1), 348-360. https://doi.org/10.58346/JISIS.2025.I1.022

[3] Al-Kadhimi, A. A., Singh, M. M., & Khalid, M. N. A. (2023). A systematic literature review and a conceptual framework proposition for advanced persistent threats (apt) detection for mobile devices using artificial intelligence techniques. *Applied sciences*, *13*(14), 8056. https://doi.org/10.3390/app13148056

[4] Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), 11-27. https://doi.org/10.7753/IJCATR1308.1002

[5] Aramide, O. O. (2023). Predictive Analytics and Automated Threat Hunting: The Next Frontier in AI-Powered Cyber Defense. *International Journal of Technology, Management and Humanities*, *9*(04), 72-93. https://dx.doi.org/10.21590/ijtmh.2023090407

[6] Asad, F., & Steltzer, H. (2025). Artificial Intelligence in Cyber Defense: Predicting and Preventing Cyber Threats.

[7] Capa, K. A. (2024). The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems. *Security Issues, (1)*, 61-70.

[8] Chopra, N., & Patil, V. (2025). *Design of advancements in AI for cyber threat detection*. In *Essentials in cyber defence* (pp. 16–34). Periodic Series in Multidisciplinary Studies.

[9] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920

[10] De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial intelligence and the future of defense: strategic implications for small-and medium-sized force providers*. The Hague Centre for Strategic Studies.

[11] Falowo, O. I., Botsyoe, L. E., Koshoedo, K., & Ozer, M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. *IEEE Access*, *12*, 123811-123822. https://doi.org/10.1109/ACCESS.2024.3454543

[12] Hasan, K., Shetty, S., & Ullah, S. (2019, December). Artificial intelligence empowered cyber threat detection and protection for power utilities. In *2019 IEEE 5th international conference*

on collaboration and internet computing (CIC) (pp. 354-359). IEEE. https://doi.org/10.1109/CIC48465.2019.00049

[13] Hoa, N. T., & Voznak, M. (2025). Critical review on understanding cyber security threats. *Innovative Reviews in E*ngineering and Science, 2(2), 17-24.

[14] Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B., & Okolo, J. N. (2025). Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches. *International Journal of Scientific Research and Modern Technology*, *4*(3), 1-15. https://doi.org/10.38124/ijsrmt.v4i3.376

[15] Khalid, M. N. A., Al-Kadhimi, A. A., & Singh, M. M. (2023). Recent developments in game-theory approaches for the detection and defense against advanced persistent threats (APTs): a systematic review. *Mathematics*, *11*(6), 1353. https://doi.org/10.3390/math11061353

[16] Khan, W., Ashoka, K., Razak, M. A., Kumar, M. M., & Naseer, R. (2025). A Comprehensive Survey on Cognitive Cyber Security Analysis using Machine Learning Approaches. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3614388

[17] Kolade, T. M., Obioha Val, O., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-driven open-source intelligence in cyber defense: A double-edged sword for national security. *Adebayo Yusuf and Gbadebo, Michael Olayinka and Olaniyi, Oluwaseun Oladeji, AI-Driven Open-Source Intelligence in Cyber Defense: A Double-edged Sword for National Security (January 18, 2025)*.

[18] Kreinbrink, J. L. (2019). *Analysis of artificial intelligence (AI) enhanced technologies in support of cyber defense: Advantages, challenges, and considerations for future deployment* (Master's thesis, Utica College).

[19] McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Ng, A., & Halgamuge, M. N. (2024). A game-theoretic approach to containing artificial general intelligence: Insights from highly autonomous aggressive malware. *IEEE Transactions on Artificial Intelligence*, *5*(12), 6290-6303. https://doi.org/10.1109/TAI.2024.3394392

[20] Mehra, A., & Iyer, R. (2021). Improving Cybersecurity Using Artificial Intelligence: Overview, Modeling, Future Directions. *International Academic Journal of Science and Engineering, 8*(2), 11–15.

[21] Pleshakova, E., Osipov, A., Gataullin, S., Gataullin, T., & Vasilakos, A. (2024). Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. *Journal of Computer Virology and Hacking Techniques*, *20*(3), 429-440. https://doi.org/10.1007/s11416-024-00529-x

[22] Raji, A., Olawore, A., Mustapha, A., & Joseph, J. (2023). Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. *World Journal of Advanced Research and Reviews, 20*(3), 2005-2024. https://doi.org/10.30574/wjarr.2023.20.3.2741

[23] Randieri, C., & Tomazzoli, C. (2025). Advancing Cyber Defense with Artificial Intelligence: State-of-the-Art Techniques and Future Directions. In *Advancements in Cybersecurity* (pp. 503-526). CRC Press.

[24] Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., & Tian, Z. (2022). CSKG4APT: A cybersecurity knowledge graph for advanced persistent threat organization attribution. *IEEE Transactions on Knowledge and Data Engineering*, *35*(6), 5695-5709. https://doi.org/10.1109/TKDE.2022.3175719

[25] Siddiqui, S. (2016). Cognitive artificial intelligence–a complexity-based machine learning approach for advanced cyber threats.

[26] Sumari, A. D. W., Setiawan, A., & Syamsiana, I. N. (2020). Cognitive artificial intelligence application to cyber defense. In *IOP Conference Series: Materials Science and Engineering* (Vol. 732, No. 1, p. 012037). IOP Publishing. https://doi.org/10.1088/1757-899X/732/1/012037

[27] Trim, P. R., & Lee, Y. I. (2022). Combining sociocultural intelligence with Artificial Intelligence to increase organizational cyber security provision through enhanced resilience. *Big Data and Cognitive Computing*, *6*(4), 110. https://doi.org/10.3390/bdcc6040110

[28] Udaya kumar, R., Joshi, A., Boomiga, S. S., Sugumar R. (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification. *Journal of Internet Services and Information Security*, *13*(4), 138-157. https://doi.org/10.58346/JISIS.2023.I4.010

[29] Yenduri, G., Murugan, R., Maddikunta, P. K. R., Bhattacharya, S., Sudheer, D., & Savarala, B. B. (2025). Artificial general intelligence: Advancements, challenges, and future directions in AGI research. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3592708

Authors Biography

Akash Parasumanna Sridhar is a Security Engineer at Campbell Clinic Orthopaedics in Memphis, Tennessee, where he leads initiatives in threat detection, incident response, and security architecture. He actively monitors and responds to real-time cyber threats, analyzes cross-platform logs, and strengthens organizational defenses through detection engineering and automation. With expertise in both blue and red teaming, Akash has conducted reconnaissance, exploitation, and social engineering assessments to enhance organizational resilience. He holds a Master's degree in Cybersecurity from the University of Houston and is a published researcher and conference speaker, known for sharing practical insights on building resilient healthcare security systems. He holds multiple industry certifications, including CEH v11, CHFI, eJPTv2, Pentest+, CCNA, SC-200, Security+, Cloud+, CySA+, CASP+, SecurityX, and is also a Certified EC-Council Instructor—demonstrating his breadth across offensive and defensive domains in cybersecurity.