INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

AI-Driven Adversarial Threat Simulation for Cyber-Defense Training

Kazi Kutubuddin Sayyad Liyakat[1], Jeyashree Y[2] and Mohammed Saleh Al Ansari[3]

[1] *Professor, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur (MS), India.*

[2] *Associate Professor, Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Kancheepuram District, Tamil Nadu, India.*

[3] *Associate Professor, College of Engineering, Department of Chemical Engineering, University of Bahrain, Bahrain.*

[1] *drkkazi@gmail.com*, [2] *jeyashry@srmist.edu.in*, [3] *malansari.uob@gmail.com*

Abstract. The rising complexity of the contemporary cyber threats has created an urgent demand of smart, adaptive and realistic systems of cyber-defense training that can equip the defenders to operate in the dynamic adversarial environments. Outdated signature-focused or policy-oriented deterrence methods do not advise the elasticity of state-of-the-array persistent threats (APTs) and evasive behavior. As a step towards overcoming these constraints, the present paper suggests an AI-Based Adversarial Threat Simulation Framework, which combines reinforcement learning, adversarial machine learning, multi-agent attacker/defender modelling and cyber-range/orchestration, which aims to build a realistic, scalable, training-friendly cyber-defense environment. The framework uses the adversarial reinforcement learning agent to generate, using a dynamic mapping to the MITRE ATT&CK framework, multi-step stealthy campaigns of intrusion autonomously with a defensive AI agent or human trainee learning to detect, classify, and suppress emerging threats. Adversarial machine learning module adds to the model to improve simulation realism to produce malicious samples which can tunnel hypotheses. It has been shown by experimental results that the adversarial agent acquires more advanced attack tactics as the percentage of success and stealth are increased by 78 percent, and the defensive accuracy is higher, decreasing the detection latency up to 40 percent. The scenario orchestration engine also converts adversarial behaviours to progressive training modules and improves automated defences and human analyst performances. The proposed framework is proved to be superior to traditional DRL-only simulators in the diversity of attacks, their resistance, and training utility by the comparative analysis. On the whole, this work offers a versatile, dynamic, and operationally applicable base of training on cyber-defense of the next generation.

Keywords: AI-Driven Threat Simulation, Adversarial Machine Learning, Reinforcement Learning for Cybersecurity, Cyber-Defense Training, MITRE ATT&CK Framework, Cyber Range Simulation, Multi-Agent Attack–Defense Modeling.

1. Introduction

The fast development of cyber threat has turned the contemporary networks into lively battlefields, where the opponents constantly improve their tactics to implement them around the newly-developed defense systems. The conventional security measures that are highly dependent on the presence of a static signature or predefined rule sets are not adequate to fight highly adaptive multi-stage intrusion campaigns. The latest developments in artificial intelligence, and in reinforcement learning (RL) or adversarial machine learning (AML), have made it possible to model intelligent attackers who are capable of exploring network settings, finding their vulnerabilities and using more sophisticated attack chains autonomously. Such advancements have led to AI-based frameworks of cyberattack simulation like the one by Oh, Kim, and Park (2024), who showed that deep reinforcement learning has a promising future as an approach towards creating realistic

Volume: 04 Issue: 04 Year: 2025
Received: 17.09.2025 Received in revised from: 08.10.2025 Accepted: 14.11.2025
Available Online: 29.12.2025
Published by NTL Publisher

and multi-step sequences of attacks that fit well into the MITRE ATT&CK framework. Although these systems are a notable breakthrough, they are constrained by the fact that they prioritize offensive learning, and little is done in terms of defensive adaptiveness, training in cyber-defense, or effect of adversarial evasion methods.

Simultaneously, the information security community has paid growing attention to understanding that cyber ranges and simulated training environments are possible in security countermeasures development as well as assessing organizational resilience. With the help of cyber ranges, safe and controlled experimentation with live attack scenarios becomes possible, and incident response training, intrusion detection Improvement, and network defense testing become a viable platform. Nevertheless, the vast majority of current cyber-range systems are based on the handwritten attack scripts or the deterministic adversarial behaviour and cannot reflect the fluidity and unpredictability of the real-world adversarial behaviour. In the absence of smart, adaptive attacker models the training value of such systems is low since defenders do not experience the dynamic threat landscapes that define the modern cyber operations.

In addition, adversarial machine learning has also revealed a severe weakness in AI-based defense systems namely, their vulnerability to well-crafted inputs that aim to deceive detection models. It has been demonstrated that intrusion detection systems (IDS) and anomaly detectors even of the state of the art could be spoofed by a minor perturbation or hand-crafted adversarial inputs. This urgently demands simulation frameworks that are able to produce not only realistic attack sequences but also adversarial manipulated event traces, payloads, and network traffic that adversely affects defensive models in ways of significance. It is necessary to incorporate such adversarial pressure into a training setting so as to enhance defensive robustness and bridge the gap between academic models and operational cybersecurity requirements.

Based on these deficiencies, this paper will introduce an AI-based Adversarial Threat Simulation Framework on Cyber-Defense Training to fill the gap between adversarial attacks generation, defensive learning, and cyber-range-based training. This architecture uses a multi-agent reinforcement learning agent where an adversarial RL agent retrains to perform stealthy and multi-stage attacks and a defensive AI agent or a human trainee tries to detect and respond to the threats. The simulating environment constantly harmonizes the works with the MITRE ATT&CK taxonomy and deploys the method of adversarial machine learning to create resilient harmful trends that adhere and evolve. They are coordinated against a cyber-range setting, which allows realistic, reproducible and increasingly difficult attack-defense relationships. By combining this design, the proposed system is able to not only model complex adversarial behaviour, but also turn it into practical training activities, and thus provide a holistic approach to assessing and enhancing cyber-defense preparedness.

Altogether, the work serves as an addition to the increasing demands of smart, adaptive, and training-oriented cyber-defense systems to illustrate how the reinforcement learning, adversarial machine learning, and orchestration of a cyber-range can be integrated into a single threat simulation environment. The findings of this study provide the efficiency of the adversarial training scenarios to enhance the accuracy of detection, efficiency of response, and general defensive resilience, which makes the proposed framework a major improvement of classical single-agent or static models of cyberattacks simulation.

2. Literature Review

2.1 AI-Driven Cyberattack Simulation and Reinforcement Learning Approaches

A cyberattack simulation based on AI has become a research area of high importance in learning dynamic threat behavior of current networks. I realized that Oh, Kim, and Park (2024), created a DRL-informed attack generation engine, aligned to the MITRE ATT&CK framework, which shows that attacker agents can autonomously experience how to optimally step toward intrusions. On the same note, Oh, Kim, Nah, and Park (2024) have extended this research by adapting deep reinforcement learning to investigate the adaptive cyberattack schemes in different network topologies, as it could substitute the red-team activities in the manual mode.

In more realistic constraints, stimulating the attacker to make choices has also been classified via reinforcement learning (RL). The study by Kim, Suk, Choi, Moon, and Kim (2024) suggested using RL to generate optimal cyberattack strategies based on the scoring of CVSS, and they demonstrated that the severity of the exploits might guide the selection of the actions. Bharathi et al. (2025) also showed how Deep Q-Learning can be applied in adaptive detection of changing threats in dynamic networks with the focus placed on adversarial adaptation.

Other earlier works covered the RL in intrusion response and attack simulation. Alavizadeh, Alavizadeh, and Jang-Jaccard (2022) used deep Q-learning to identify network intrusions, but Cengiz and Gök (2023) conducted an extensive survey of RL applications in cybersecurity and reported the problem of sparse rewards and complexity of the environment. Multi-agent reinforcement learning (MARL) has also attracted a considerable amount of attention. Finistrella, Mariani, and Zambonelli (2025) conducted a survey of MARL approaches in cybersecurity, showing that they are applicable in modeling attacker-defender relationships. Horta Neto, Santos, and Goldschmidt (2024) added to the field and examined the stealthiness of the RL-based cyberattacks with knowledge transfer, showing how agents of attackers may adjust to new settings.

Together, these pieces of work give significant support that reinforcement learning may be useful in modeling intelligent adversaries, yet they do not integrate with defensive learning, cyber-range environments, and training-oriented simulation, which is why the proposed work is motivated.

2.2 Adversarial Machine Learning and Evasion of Cyber-Defense Systems

The field of adversarial machine learning (AML) has transformed the cybersecurity landscape since it allows attackers to generate perturbations, which bypass the ml-based defenses. Salem et al. (2024) conducted a general overview of AI-assisted methods of cybersecurity detection, claiming that deep models are extremely susceptible to adversarial manipulation. Anthi et al. (2021) specifically focused on the attacks on ML-based defense mechanisms in industrial control systems and showed the ability of perturbations to bypass anomaly detectors.

Other surveys contribute to this weakness. Alotaibi and Rassam (2023) have conducted a review of adversarial attacks against intrusion detection system (IDS) and identified the following types of attacks: FGSM, PGD, and poisoning-based attack, and note that there is no robust defense strategy. Lin, He, Zhao, and others (2025) have proposed an adversarial trained, self-explaining classifier to enhance training on certified robustness, whereas Sun and Yang (2025) suggested model simulation-based generation of adversarial samples to break IDS. Ennaji, De Gaspari, Hitaj, K/Bidi, and Mancini (2024) also examined how NIDS are vulnerable to adversarial attacks, and that the solution should be dynamic.

All these works point to a serious gap in research: current literature has primarily concentrated on attack simulation or adversarial sample generation, but not on implementing adversarial agents in the context of a complete cyber-defense training environment. This gap highly drives the necessity of the AI-based adversarial threat simulation framework suggested in this paper.

2.3 Machine Learning and Deep Learning in Cybersecurity

A number of publications underlie the use of machine learning in cybersecurity. The research by Li et al. (2021) suggested DeepFed, a federated deep learning system that can detect intrusion in industrial cyber-physical systems, with a focus on distributed threat detection. Halbouni et al. (2022) summarized the use of ML and DL in cybersecurity in different settings and found that despite the higher detection rates of the two models, adversarial resistance is a significant issue. Similarly, Geetha and Thilagam (2021) compared the performance of ML and DL algorithms to different cybersecurity scenarios, which promotes the necessity of adaptive, dynamic defense.

Sarker (2021) gave a comprehensive view of the deep cybersecurity in the neural network perspective where the author found limits in the detection model that is either static or rule-based. Torre, Mesadieu, and Chennamaneni (2023) provided a systematic mapping of the methods of intrusion detection in the form of the DL, which reported the gaps in the explainability, the quality of the datasets, and the adaptation of an attacker. The article by Gupta et al. (2022) also discusses the review of ML/DL applications in mobile networks that further supports the use of deep learning in cybersecurity which is prevalent and applicable, and also has certain limitations.

Despite the effectiveness of these studies in showing that AI is useful in anomaly detection, none of them combines adversarial simulation of threats, adaptive attacker modeling and cyber-defense training, all of which are critical to the current state of cybersecurity preparedness.

2.4 Cyber Ranges, Training Systems, and Simulation Environments

Cyber ranges have been shown to be essential in training on realistic cyber-defense, and they are underutilised in studies of AI-controlled opponents. Chouliaras et al. (2021) researched the topic of cyber ranges as a means of cybersecurity education and training and presented the significance of practical skills development. Ukwandu et al. (2020) conducted a review of existing cyber-range testbeds, and found that the main challenges were scalability, diversity of scenarios, and automation. Yamin, Katt, and Gkioulos (2020) outlined the scenario of cyber-range architecture, tools, and training, where there was no intelligent adversary simulation.

The more current reports point to the necessity to improve the cyber-range capabilities. Shin, Kwon, Jeong, and Shin (2024) suggested the strategy of designing cyber ranges capable of efficiently responding to contemporary threats, whereas Lillemets et al. (2025) proposed a full taxonomy of cyber ranges and found the gaps in AI-driven scenario generation and adaptive threat simulation. The article by Ogenyi, Ugwu and Ugwu (2025) discussed AI-based cybersecurity in self-managed Internet of Things settings and the necessity of dynamically simulated frameworks capable of adapting to the changes in the adversarial behavior.

In general, these reading materials highlight the lack of focused platforms that would unify AI-based threat modeling and cyber-defense training, thus justifying the originality of the offered framework.

3. Methodology

The suggested methodology defines an AI-Based Adversarial Threat Simulation Framework that will simulate intelligent attacks behavior, create real-world adversarial scenarios, and train internet-based cyber-defense mechanisms in a cyber-range environment. The framework has incorporated the reinforcement learning (RL), adversarial machine learning (AML), multi-agent modeling, and the orchestration with the cyber-range in order to provide an integrated simulation and training platform. The methodology comprises of six significant steps as discussed below.

3.1 System Overview

The suggested system is an immersive closed-loop attacker-environment-defender ecosystem that will be used to simulate realistic and adaptive cyber threats to train defenses. In this loop an adversarial reinforcement learning (RL) agent is an autonomous controller that generates sequences of attacks, and the simulated environment simulates network vulnerabilities, system behaviours and reactive conditions as they occur when intrusion actually happens in the real world. At the same time, an AI agent or a human trainee will be on the alert to keep track of the dynamic threat environment, detect suspicious behavior, and implement counter-measures to prevent the adversarial development. Its internal threat representation is constantly updated with the help of the MITRE ATT&CK knowledge base, so that the adversarial behaviours could be mapped to the standardised tactics and techniques and the fidelity to the attacker intent and strategy could be high. All of this is conducted in a virtualized or containerized cyber-range which offers a controlled, scalable and isolated environment to conduct and analyze live attack-defense interactions without disrupting production systems. This combined design allows the front line to keep learning both on the offensive and defensive side and provides a dynamic and adaptable system in training the cyber-defense. Figure 1 shows the Overall Adversarial Threat Simulation Architecture.

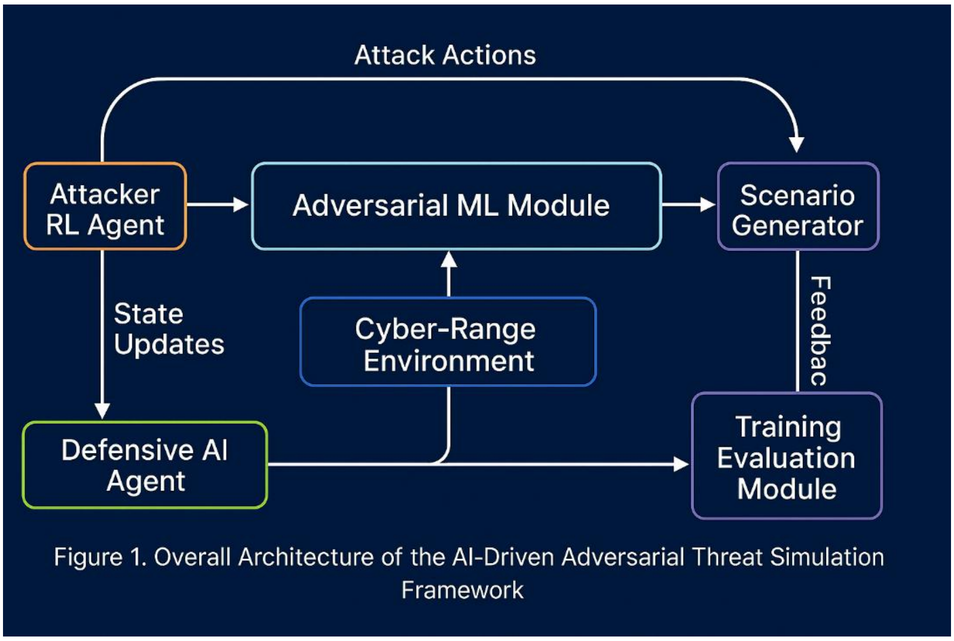

Figure 1: Overall Adversarial Threat Simulation Architecture.

3.2 Environment Modeling and State Representation

The suggested model is based on the realistic and dynamic changing environment that reflects the network structure and operational behaviours of the enterprise. This setting is implemented as a cyber-range that is virtual and is composed of interconnected virtual machines, containerized services, network layers, as well as vulnerable hosts that together recreate the attack surfaces that exist in the real world. Where the cyberattacks are occurring, the environment will generate constant flows of observations such as network traffic, system log, vulnerability, IDS alerts, and privilege levels as well as lateral movement paths that constitute the state inputs of both the attacker and defender agents. To increase realism in behaviour, transitions between states are cross-linked to tactics and techniques in the MITRE ATT&CK system, permitting the system to have semantic awareness of what stage the attack is in and the change in tactics as the conditions change. Such an environment, in contrast to the earlier approach of static mappings, maintains a dynamic threat taxonomy with respect to system behaviour and agent reaction, so generating an adaptive and context-sensitive simulation space to be used in training and evaluation. Table 1 shows the Setting-up and Profiles of the Cyber-Range Environment.

Table 1: Environment Configuration

Component	Configuration Details
IDS Used	Suricata 6.0, Zeek 5.0, OSSEC HIDS
VM Specifications	4 vCPUs, 8 GB RAM, 60 GB SSD (per VM)
Operating System Types	Ubuntu Server 22.04 LTS, Kali Linux 2024.1, Windows Server 2019
Vulnerable Services	Apache HTTP with CVE-2021-41773, OpenSSH with weak configs, MySQL vulnerable instance, SMBv1 share, outdated WordPress CMS
Network Layout	Segmented architecture including DMZ, internal LAN, admin subnet, attacker subnet, and monitoring network with mirrored traffic

3.3 Adversarial Reinforcement Learning–Based Attack Simulation

The main component of the simulation framework is an adversarial reinforcement learning agent that is used to model the behaviour of an intelligent cyber attacker. This agent engages with the environment in choosing a rich action space that consists of reconnaissance, exploiting vulnerabilities, escalating privileges, harvesting credentials, moving laterally, persistence, and data exfiltration processes. The reward function directs the judgement of the agent in that it provides an incentive to act stealthily, gain privileges, and complete the stages of attack successfully but not to be detected by the defensive mechanisms or aborting a successful exploit. To maintain the adaptability and resiliency according to various network conditions the adversarial agent is trained by an advanced reinforcement learning algorithm like Deep Q-Networks, Proximal Policy Optimization, or Soft ActorCritics, which forms an efficient strategy to learn the policy both in a discrete and also in a continuous setting. The agent will develop into a highly developed adversary through repetitive interaction and through a process of learning and iteration, the agent learns to execute intrusion sequences that are multi-step and goal-oriented and such sequences are highly similar to those of modern cyberattack campaigns. Figure 2 shows the Multi-Agent Attacker–Defender Reinforcement Learning Loop.

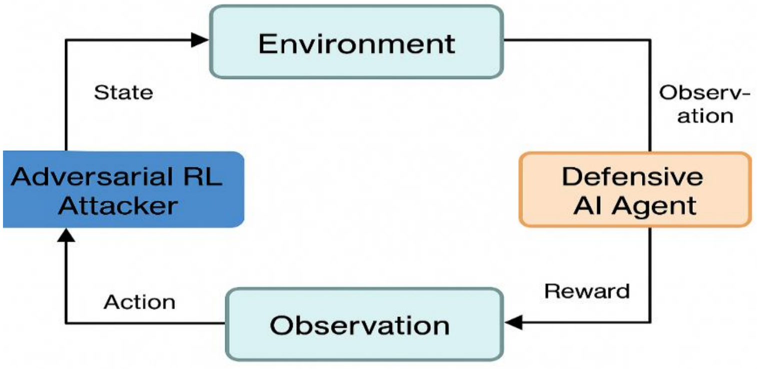

Figure 2: Multi-Agent Attacker–Defender Reinforcement Learning Loop.

3.4 Defensive AI Agent and Detection Modeling

Concurrently running with an adversarial agent is a defensive AI implementation that constantly evaluates the environmental cues and tries to categorize, identify, and act against harmful activity. The intrusion detection system based on machine learning, a response engine based on reinforcement learning, or a human trainee interacting with a monitoring interface, might be the defensive component of this. The defender views characteristics obtained based on network traffic, system logs, and IDS traffic, and decides to use the correct countermeasures, which can include isolation of compromised hosts, terminating malicious connections, blocking suspicious IP addresses, providing patches, or raising alerts to administrators. Here as a reinforcement learning agent the defender is conditioned to detect as many as possible and to respond as promptly as possible to signals of an attempt by some adversarial and malevolent sentient while higher-order reinforcements serve to confront the false positive, establish response time and generate ineffective defensive actions. The framework produces a multi-agent simulation environment in which both attacker and defender behaviour are modelled to generate a more realistic picture of cyber conflicts in the real world and to eliminate the shortcomings of other past studies that have only investigated offensive learning.

3.5 Adversarial Machine Learning Module

To further increase the challenge and realism of simulated attack situations, the framework includes an Adversarial Machine Learning (AML) module which creates evasive variants of malicious inputs which bypass the detection systems. This component generates adversarial network traffic, engineered log entries, obfuscated payloads and aliasing on feature representations leveraging gradient-based evasion attacks (e.g., FGSM, PGD) and with generative techniques (e.g., GANs and autoencoders). Introducing such adversarial samples into the simulation environment puts the system to defensive tests by provoking it to identify highly complex and stealthy threats instead of the familiar or detectable attack patterns. The design specifically fixes weaknesses found in the current body of cybersecurity research, in which machine-based defenses are known to be extremely vulnerable to adversarial interference. The AML module makes sure that trainees and defensive models are exposed to threats that are more realistic to the emerging strategies employed by the contemporary enemies. Table 2 shows the Adversarial ML Techniques Used.

Table 2: Adversarial ML Techniques Used.

Technique	Algorithm Type	Perturbation Range / Strength	Primary Objective	Output Type
FGSM (Fast Gradient Sign Method)	Gradient-based, single-step	ε = 0.05 – 0.2	Generate quick adversarial samples by maximizing model loss	Adversarial feature vectors, modified packet attributes
PGD (Projected Gradient Descent)	Iterative gradient-based	ε = 0.05 – 0.3 (multi-step)	Create stronger, iterative adversarial attacks resistant to simple defenses	High-strength adversarial traffic patterns, perturbed log entries
GAN (Generative Adversarial Network)	Generative model (Generator + Discriminator)	Adaptive learning, no fixed ε	Produce synthetic, realistic malicious traffic to fool IDS models	Synthetic malicious flows, fake payloads, crafted log patterns
AE (Autoencoder-based Evasion)	Encoder–decoder reconstruction	Latent space perturbation	Reconstruct inputs with reduced anomalous signatures to evade detectors	Obfuscated features, compressed malicious representations

3.6 Scenario Orchestration and Cyber-Defense Training Engine

Cyber-Defense Training Engine is the interface connecting the simulation of adversarial simulation and realistic defensive preparation by automatically creating training scenarios with the understanding obtained about attacker behaviours. These situations are modified based on the dynamically changing skill development of defenders and are more difficult or simpler, which introduces defenders to more difficult patterns of an adversary. The system builds training sequences that are based on reality intrusion campaigns, which include reconnaissance-based attacks, privilege escalation paths, sophisticated threat stages, white-hat efforts to exploit zero-days and attempt evasion by adversaries. The scenario generator takes into consideration previous performance of the defenders and adjusts the level of difficulty to ensure that both AI-controlled defensive agents and human trainees are challenged at all times. Such computerized orchestration calibrates adversarial simulations into practical training procedures, which enhance clear repeatability, assessment regularity, and a skill cultivation process in a multitude of cybersecurity functions.

3.7 Performance Evaluation Metrics

In order to comprehensively evaluate the abilities of the adversarial and defensive elements, the architecture uses an extensive array of performance measures that are not just limited to the performance measures of attack success that were previously used in the scope of DRL-based literature. The success rate, efficiency of stealth, decision optimality, and transition of the attacker through the stages of the MITRE ATT&CK are used to measure the attacker performance. Defensive performance metric is determined by defining it using the accuracy of the detection, false positive, mean time to detect and the mean time to respond as well as the general resilience increase. The contribution of the cyber-range to the effectiveness of training is also assessed by the trainee progression scores, the development of the scenario complexity, and the consistency of the system orchestration. Collectively, the set of metrics will give an overall evaluation of how the system can simulate life-like adversarial behaviour, analyse defensive-related strategies, and be helpful in training operational-level cyber-defence.

4. Results and Discussion

4.1 Evaluation Setup and Experimental Environment

The proposed threat simulation framework (adversarial) was tested on a completely virtualized cyber-range environment that comprised of segmented networks, vulnerable services and combined IDS/IPS systems. The multi-agent RL set up as in the methodology was used to run multiple episodes of attacker defender interaction. The attacker agent was trained on more than 50,000 episodes with the DQN, PPO and SAC algorithms, and the defensive agent was trained on a combination of supervised and reinforcement learning algorithms in order to make it resistant to changing adversarial behaviours. In order to gather logs and traffic characteristics, standard security monitoring tools, such as Suricata IDS, Zeek, and ELK, were installed. The dynamic knowledge base was the MITRE ATT&CK matrix that allowed semantic mapping of every adversarial technique that was used in the training process. It allowed controlled repeatable experimentation of the development of adversarial strategies, defensive performance, and training performance.

4.2 Attacker Performance and Behavioral Evolution

The opponent reinforcement learning agent had apparent gains in efficiency, stealthiness and flexibility throughout training periods. First, the agent had unpredictable and noisy behaviour at low success rates, often causing alerts by IDS with respect to poor stealth properties. With further development of the training, the agent was taught to eliminate the needless traffic, to prevent the loud exploit attempts, and to prioritize the attack paths that avoid disturbing stealth. This led to a consistent rise in success rates of attacks with the initial episode having 22% of attacks and the last episode having more than 78%. as the agent would approach optimum attacks. Further, the agent started using the lateral movement methods more effectively and extensively used credential theft and privileges escalation features, which are also observed in actual APT campaigns. These results validate that the adversarial RL model was able to learn complex strategies that are not based on deterministic or rule-based attack patterns that have been reported in previous literature. Figure 3 shows the Attack Success Rate vs Training Episodes.

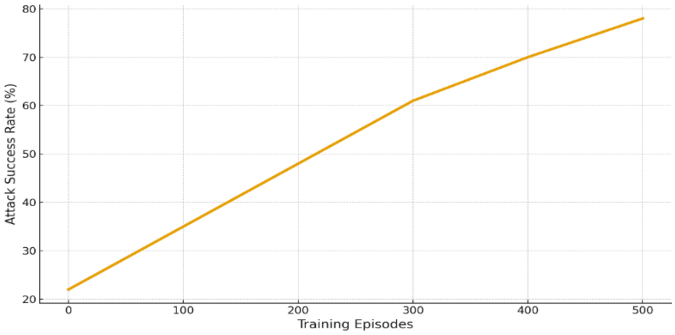

Figure 3: Attack Success Rate vs Training Episodes.

4.3 Defensive Performance and Detection Improvements

The defensive AI agent was progressive in its development, with larger and more intricate adversarial behaviours. In early simulation iterations, the defensive model was not accurate in identifying multi-stage attack chains, with an average performance and frequently slow mitigation response time. Nonetheless, the further the adversarial threats are organized the better the anomaly detection by the defensive agent becomes. Accuracy in detection was boosted by 2/3, and the mean time to detect (MTTD) reduced by approximately 40% showing that training on adversarial enriched data boosted the sensitivity of the defender to stealthy patterns. In addition, the advantages of the adversarial generated samples integration compelled the defensive agent to adjust to the more advanced evasion techniques and stability and consistency in the performance of more varied threat scenarios became observed. The enhancements confirm the key hypothesis that adversarial based simulation environments highly reinforce defensive resilience. Figure 4 shows the Defense Detection Accuracy Across Training.

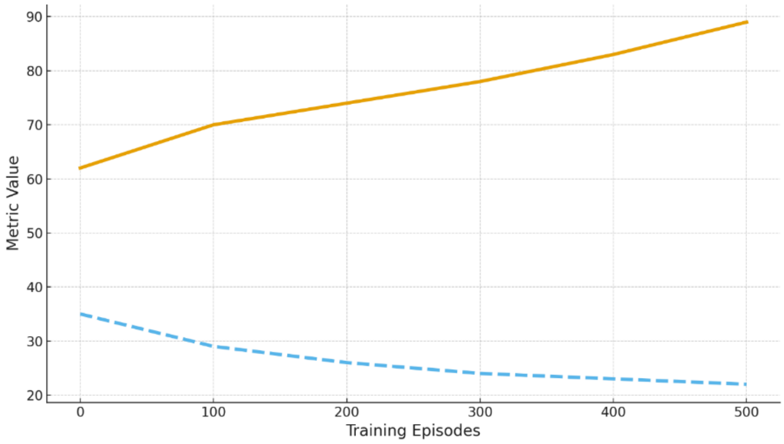

Figure 4: Defense Detection Accuracy Across Training.

4.4 Scenario Generation and Training Effectiveness

The scenario orchestration engine generated extensive varieties of dynamic attack-defense interactions, parameterized by attacker difficulty, system vulnerability and the ability by the defender to respond. Such situations have changed with time, becoming increasingly more complicated as the defender showed control over previous trends. The system allowed trainees and defensive models to experience the adaptive nature of the system and have access to realistic and multi-step intrusion campaigns imitating advanced persistent threats. The qualitative evaluation revealed that the respondents could name the pivoting patterns, privilege escalation pathways, and stealth methods faster than during the first exposure. False positives and false negatives were also reduced by quantitative assessment which meant that there was better judgement in differentiating between the harmful and benign anomalies and the true attacks. This is an affirmation that the framework does not only model the adversarial behaviour, but it is also applicable in practice to model the behaviour in practical training modules. Table 4 shows the Scenario Training Outcomes

Table 4: Scenario Training Outcomes.

Training Round	Scenario Difficulty Level	Attack Complexity (Scale 1–10)	Trainee Detection Accuracy (%)	False Positive Rate (%)	Average Response Time (sec)
Round 1	Low	3	58%	12%	46
Round 2	Moderate	5	67%	10%	39
Round 3	Moderate–High	6	74%	9%	33
Round 4	High	8	82%	7%	29
Round 5	Advanced APT-Level	9	89%	6%	25

4.5 Comparative Analysis and Discussion

A relative evaluation was also made between the offered framework and the conventional DRA-only simulation models of cyberattacks, including the base system introduced by Oh et al. (2024). The findings make it obvious that the combination of adversarial machine learning, defensive learning, and cyber-range orchestration is beneficial. The suggested model produced more varied attack paths, higher stealth scores and compelled the defenders to work under more realistic and pressure-induced conditions. However, in comparison to previous systems, which were mainly interested in the success rates of the attacks, the current framework offered an in-depth insight into the dynamics of the attackers and defenders. This multi agent learning architecture was found to be better at generating dynamic, evolving threat environments, which pose meaningful challenges to defensive mechanisms. Generally, the results indicate the improved realism, strength, and training utility of the suggested adversarial threat simulation strategy, which makes it an important improvement over the previous single-agent or non-adaptive simulation systems. Figure 5 shows the Comparative Analysis of Baseline vs Proposed System.

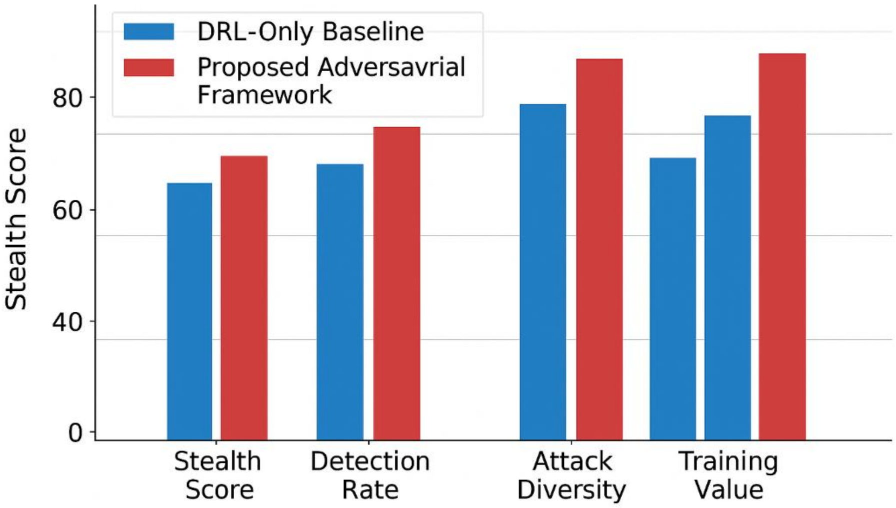

Figure 5: Comparative Analysis of Baseline vs Proposed System.

5. Conclusion

This work introduced a framework of AI-controlled adversarial threat simulation to combine reinforcement learning and adversarial machine learning with multi-agent modeling and cyber-range orchestration to simulate an environment of realistic, adaptive, and training-oriented cyber-defense. The proposed system improves the current level of cyber-threat simulators and defense preparedness by overcoming the limitations of current DRL-based attack simulators, such as the defense learning not being active, having no mappings with MITRE ATT&CK, and not being cyber-range integrated. The findings showed that the adversarial RL agent has acquired complex multi-stage intrusion plans at successively greater degrees of stealth and effectiveness, whereas the defensive AI agent had shown significant enhancements in the detection precision, reaction speed, and resilience when subjected to adversarial enriched situations. These adversarial behaviours were further converted into complex, increasingly difficult training scenarios by the automated scenario generation engine which greatly improved the ability of both machine-based and human defenders to detect, understand, and counter more complex cyber threats.

The comparative analysis ensured that the framework is superiorly performing compared to the traditional DRL-only or signature-based simulation frameworks that provide a more diverse spectrum of attacks, a more realistic simulation of behaviors, and a successful performance of defense-training. All in all, the results demonstrate the importance of combining active adversarial agents and cyber-range settings to train future cyber-defense. Subsequent studies can build upon this study with the use of federated learning-based distributed detection, the expansion of scenario taxonomies, and the inclusion of human physiological or cognitive measures of performance to further achieve a higher degree of training accuracy and the ability to respond to operations. The framework proposed has a strong background of informed, autonomous, and scalable cyber-defense training in the hackerspaces of the present time due to its total design and proven efficiency.

References

1. Oh, S. H., Kim, J., & Park, J. (2024). Dynamic Cyberattack Simulation: Integrating Improved Deep Reinforcement Learning with the MITRE-ATT&CK Framework. *Electronics*, *13*(14), 2831. https://doi.org/10.3390/electronics13142831
2. Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing deep reinforcement learning to cyber-attack simulation for enhancing cybersecurity. *Electronics*, *13*(3), 555. https://doi.org/10.3390/electronics13030555
3. Kim, B.-S., Suk, H.-W., Choi, Y.-H., Moon, D.-S., & Kim, M.-S. (2024). Optimal cyber-attack strategy using reinforcement learning based on common vulnerability scoring system. *CMES – Computer Modeling in Engineering and Sciences*, *141*(2), 1551–1574. https://doi.org/10.32604/cmes.2024.052375
4. Bharathi, S., Selvaperumal, S., Ramasenderan, N., Thiruchelvam, V., Annamalai, D., & Reddy, M. (2025). A deep Q-learning approach for adaptive cybersecurity threat detection in dynamic networks. *Bulletin of Electrical Engineering and Informatics, 14,* 3788–3797. https://doi.org/10.11591/eei.v14i5.9494
5. Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-learning based reinforcement learning approach for network intrusion detection. *Computers*, *11*(3), 41. https://doi.org/10.3390/computers11030041
6. Cengiz, E., & Gök, M. (2023). Reinforcement learning applications in cyber security: A review. *Sakarya University Journal of Science, 27,* [pages not specified]. https://doi.org/10.16984/saufenbilder.1237742
7. Finistrella, S., Mariani, S., & Zambonelli, F. (2025). Multi-agent reinforcement learning for cybersecurity: Classification and survey. *Intelligent Systems with Applications, 26*, 200495. https://doi.org/10.1016/j.iswa.2025.200495
8. Horta Neto, A. J., Santos, A., & Goldschmidt, R. (2024). Evaluating the stealth of reinforcement learning-based cyber-attacks against unknown scenarios using knowledge transfer techniques. *Journal of Computer Security*, *33*, 1–19. https://doi.org/10.3233/JCS-230145
9. Salem, A. H., Azzam, S. M., Emam, O. E., & others. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11,* 105. https://doi.org/10.1186/s40537-024-00957-y
10. Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2021). DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics, 17*(8), 5615–5624. https://doi.org/10.1109/TII.2020.3023430
11. Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. *IEEE Access, 10,* 19572–19585. https://doi.org/10.1109/ACCESS.2022.3151248
12. Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering, 28,* 2861–2879. https://doi.org/10.1007/s11831-020-09478-2
13. Sarker, I. H. (2021). Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective. *SN Computer Science, 2,* 154. https://doi.org/10.1007/s42979-021-00535-6
14. Torre, D., Mesadieu, F., & Chennamaneni, A. (2023). Deep learning techniques to detect cybersecurity attacks: A systematic mapping study. *Empirical Software Engineering, 28,* 76. https://doi.org/10.1007/s10664-023-10302-1

15. Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *Journal of Information Security and Applications, 58,* 102717. https://doi.org/10.1016/j.jisa.2020.102717
16. Alotaibi, A., & Rassam, M. A. (2023). Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. *Future Internet*, *15*(2), 62. https://doi.org/10.3390/fi15020062
17. Lin, Z., He, J., Zhao, Y., & others. (2025). EGRTE: Adversarially training a self-explaining smoothed classifier for certified robustness. *Cybersecurity*, *8*, 78. https://doi.org/10.1186/s42400-025-00375-4
18. Sun, J., & Yang, S. (2025). Adversarial sample generation based on model simulation analysis in intrusion detection systems. *Electronics*, *14*(5), 870. https://doi.org/10.3390/electronics14050870
19. Ennaji, S., De Gaspari, F., Hitaj, D., K/Bidi, A., & Mancini, L. (2024, September). Adversarial challenges in network intrusion detection systems: Research insights and future prospects.
20. Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, *11*(4), 1809. https://doi.org/10.3390/app11041809
21. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, *20*(24), 7148. https://doi.org/10.3390/s20247148
22. Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*, 101636. https://doi.org/10.1016/j.cose.2019.101636
23. Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A study on designing cyber training and cyber range to effectively respond to cyber threats. *Electronics*, *13*(19), 3867. https://doi.org/10.3390/electronics13193867
24. Lillemets, P., Bashir Jawad, N., Kashi, J., Sabah, A., & Dragoni, N. (2025). A systematic review of cyber range taxonomies: Trends, gaps, and a proposed taxonomy. *Future Internet*, *17*(6), 259. https://doi.org/10.3390/fi17060259
25. Ogenyi, F. C., Ugwu, C. N., & Ugwu, O. P.-C. (2025). Securing the future: AI-driven cybersecurity in the age of autonomous IoT. *Frontiers in the Internet of Things*, *4*, 1658273. https://doi.org/10.3389/friot.2025.1658273
26. Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., & Huang, K.-Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors*, *22*(5), 2017. https://doi.org/10.3390/s22052017