

AUTONOMOUS CYBER DEFENSE: INTELLIGENT THREAT DETECTION, RESPONSE, AND RECOVERY IN DYNAMIC NETWORK ENVIRONMENTS

Sufyan Ashraf Khan^{*1}, Dr. Imran Khan², Sohaib Rasheed Bhatti³, Mahnoor Siddique⁴

^{*1}Researcher, Computer System Engineering, Mirpur University of Science and Technology

²Assistant Professor, Department of Artificial Intelligence, Dawood University of Engineering and Technology

³Student, Department of Software Engineering, NUST, MCS Rawalpindi

⁴Department of Computer Science, UET Lahore

^{*1}sufyanashrafkhan@gmail.com, ²imran.khan@duet.edu.pk, ³pathfinder7545@gmail.com

⁴mahnoorsiddique94@gmail.com

DOI: <https://doi.org/10.5281/zenodo.22930517>

Keywords

Adaptive Recovery, Automated Incident Response, Autonomous Cyber Defense, Cybersecurity, Intelligent Threat Detection, Network Security

Article History

Received: 01 June 2026

Accepted: 23 August 2026

Published: 24 September 2026

Copyright @Author

Corresponding Author: *

Sufyan Ashraf Khan

Abstract

The study focused on autonomous cyber defense being adopted as an umbrella of smart threat detection, intelligent incident response, and resilient recovery in evolving network settings. A quantitative research design was adopted in the study to explore the relationship between Intelligent Threat Detection (ITD), Automated Incident Response (AIR), Adaptive Recovery (AR), and Autonomous Cyber Defense (ACD). A total of 300 respondents completed a structured questionnaire with a 5-point Likert scale to provide the data for this study, comprising cybersecurity professionals and IT practitioners. The data were analyzed using descriptive statistics, Pearson correlation and multiple linear regression. The results showed that the Intelligent Threat Detection had a significant and positive effect on the Autonomous Cyber Defense ($\beta = 0.42$, $p < .001$). Additionally, Automated Incident Response had a strong positive correlation with Autonomous Cyber Defense ($\beta = 0.31$, $p < .001$) and Adaptive Recovery had a strong positive correlation with Autonomous Cyber Defense ($\beta = 0.27$, $p < .001$). The overall regression model was statistically significant, $R^2 = 0.584$ (Adjusted $R^2 = 0.580$, $F(3, 296) = 138.48$, $p < .001$). The results pointed to the need for incorporating intelligent detection, intelligent response, and intelligent recovery in an autonomous cybersecurity architecture. The study enhanced the understanding of the importance of synchronized defense in maintaining ongoing threat management, quick response, network resiliency and adaptation to evolving network environments.

INTRODUCTION

The advent of the Internet of Things (IoT) devices, spreadsheets of digital infrastructures, enterprise systems, and the growing mesh and proliferation of these devices, by themselves and with each other,

transformed the cybersecurity landscape and made it more difficult to defend. These attacks were increasingly dynamic, automated, had very advanced malware, moved laterally and included attack patterns that were not seen before, and

posed a challenge to the traditional “signature” based and “static” based security tools. In actively attacking and evading by using obfuscation and unknown attack patterns, Khraisat et al. (2019) pointed out that traditional IDSs have some key shortcomings. Sarker et al (2020) pointed out that the information science of cybersecurity presented the opportunity of cybersecurity decisions to be automated and intelligence by analyzing information regarding cybersecurity and uncovering meaningful patterns.

Artificial Intelligence (AI) upgraded the cybersecurity equipment to automatically detect, classify, predict and respond to threats. According to Kaur et al. (2023) AI in cybersecurity encompassed significant AI capabilities such as detection, protection, recovery and response as well, and the use of machine learning and deep learning techniques were said to be employed for handling large volumes of security information. Similarly, Salem et al. (2024) studied the AI-based detection methods and demonstrated the involvement of machine/ deep learning tools in many network scenarios for detecting cyber threats. These trends showed a shift from alert generation to investigating events and enabling quick defensive decision making. One thing of particular significance was aid in the development of deep reinforcement learning (DRL) which allows an agent to learn defence actions by interacting with an environment. The cyber environment is dynamically changing with unpredictable nature of the attacks and challenging decision making process which demands a promising solution as DRL, according to Nguyen & Reddi (2023).

This development led to the emergence of the concept of “autonomous cyber defense”, aiming to develop systems which are able to detect threats and react with proper measures, which will be able to help in recovery, with minimal involvement of a human. Autonomous cyber network defense is identified as a new cyber research domain by Vyas et al. (2025), which lies within the scope of autonomous agents, reinforcement learning, intelligent response mechanism and realistic cyber-operation environment. Also investigated was

autonomous defence systems that integrated a deep reinforcement learning framework, knowledge graphs, and LLMs, which further improved its capabilities of understanding and selecting responses in context (Loevenich et al., 2025). As can be seen, in recent years there has been renewed interest in the adoption of solutions in complex interconnected systems, including in the field of artificial intelligence autonomous defense in IoT environments, analyzed by Shi et al. (2025).

Background of the Study

The traditional cyber security systems only addressed signature-based detection, pre-defined rules and firewall policies, access control, and manually set security policies. While they were useful for identifying known threats, their effectiveness was more challenged in the face of the emergence of significant volumes of security data that were varied and rapidly changing on networks. Khraisat et al., (2019), in a recent research work, identified two general types of IDS: Signature Based and Anomaly Based, and stressed on the problem of detecting unknown and evolving attacks. With such large amounts of data in the network, deep learning was now possible—thereby allowing a computer to learn complex representations. Aldweesh et al (2020) surveyed different deep-learning techniques used by anomaly based intrusion detection and highlighted their potential use in high volume networks to support anomaly detection in complex patterns.

Another interesting feature of the autonomous cyber defence as it was developed were automated responses. Detection was good, but if the attack were after the manual investigation on alerts or action. AI systems are becoming more common with the ability to automate repetitive cybersecurity tasks, prioritize threats, and recommend and/or take action against threats. Kaur et al. (2023) stated that AI played a vital role in the detection, protection, response and recovery in the cyber security landscape. Ali and Al-Rufai (2025) explored the use of AI in

cybersecurity and discussed its various applications, such as behavioral analysis, threat intelligence, threat detection and automated response. Nguyen and Reddi (2023) pointed out the need for adaptive cybersecurity research as an approach for solving less structured and dynamic defense problems, such as DRL.

Self-defence in cyberspace also included elements of recovery – ‘effective cyber security meant not only recognising and preventing attacks’. Resilient defence was central: it needed to provide a robust defence system that would restore services, minimise damage, be able to adapt defence policies and adapt to, as well as function after, an incident. Study of self-defending and self-recovering capabilities was also gradually introduced in the fields of the intelligent security architecture as autonomous cyber defense. Morris 2025 introduced a framework of measuring the effectiveness, resilience, performance and generalizability of reinforcement-learning based cyber defense agents in the cyber arena. Vyas et al., (2025) highlighted that realistic autonomous cyber-defense environments were crucial to assessing autonomous agents under an ever-changing attack and defense scenario. In section 5, Loevenich et al. (2025) introduced the concept of combining DRL, LLM, KG, and cyber-threat intelligence into the decision-making process of defense.

Objectives of the Study

- 1.To study Intelligent Threat Detection and Autonomous Cyber Defence in dynamic network environments.
- 2.To explore the link between auto incident response and auto cyber defense.
- 3.To evaluate the connection between adaptive recovery ability and autonomous cyber defense.

Research Questions

- Q1. How was intelligent threat detection correlated with autonomous cyber defense in the dynamic network environment?
- Q2. What relationship existed between automated incident response and autonomous cyber defense?

- Q3. There was a relationship between adaptive recovery and autonomous cyber defence?

Significance of the Study

The study was important because it explored the concept of autonomous cyber defense as an all-in-one solution to the growing number of complex and evolving cyber threats. The research highlights the potential of AI in cybersecurity, emphasizing intelligent threat detection, automated incident response, and adaptive recovery, offering a comprehensive look at the role AI plays in quick and adaptive protection of network environments. The results are thought to have practical implications for cybersecurity practitioners, network administrators, security operations centers, and enterprises looking to enhance their cybersecurity defenses with intelligent automation. This study also advanced the existing body of academic research by integrating the concepts of detection, response and recovery into one overarching autonomous cyber-defense framework. The results of its work could be used in the future for research in machine learning, deep reinforcement learning, autonomous agents, threat intelligence and self-adaptive cybersecurity systems.

Research Hypotheses

- H1:** Intelligent Threat Detection significantly and positively influenced Autonomous Cyber Defense in dynamic network environments.
- H2:** Automated Incident Response significantly and positively influenced Autonomous Cyber Defense in dynamic network environments.
- H3:** Adaptive Recovery significantly and positively influenced Autonomous Cyber Defense in dynamic network environments.

Literature Review

Intelligent Threat Detection in Dynamic Network Environments

Intelligent threat detection was a key pillar of autonomous cyber defense in modern network environments, where a lot of diverse, constantly changing and huge volumes of security

information arose. Previously most IDSs were signature or rule based, which are not very effective when it comes to previously unknown or new attack patterns. Machine learning and deep learning are thus highlighted lately as learning mechanisms that can detect complex patterns in network traffic and detect anomalous traffic respectively. Ahmad et al. (2021) studied intrusion detection based on deep learning and concluded that a neural architecture provided a crucial first step in the detection of more sophisticated types of intrusions in the network environment. In spite of the benefits of supporting automatic abnormal-behavior detection in IoT networks, deep learning-based methods were found in Khan et al. (2022) to have significant challenges related to datasets, class imbalance, privacy, and model performance. There were also interests outside the classic supervised classification in the literature to move intelligent detection from supervised to reinforcement and adaptive learning. Sewak et al. (2023) explored the potential uses of DRL in the cybersecurity sector and included mention of the use of DRL in network intrusion detection, endpoint protection, IoT defense, and advanced threat protection. The reinforcement learning learned policies from the defensive agent such that it could offer a learning trial in an environment without penalties by interacting with the actions in a non-supervised way while only receiving a reward from the interactions. This particular feature was important for dynamic networks in which the attack patterns and states of network systems and defense needs changed over time. For multi-stage attacks, where the attacks and their outcomes were uncertain, Hu et al. (2020) demonstrated the use of reinforcement learning for autonomous defensive decision making by proposing an adaptive cyber-defense strategy based on a learning-based partially observable Markov decision process.

A big aspect of smart threat detection was to comprehend why the AI systems were making the decision. They may be able to recognise more intricate patterns by using complex deep-learning models and the choices the models make might be

still complicated enough to be understood by cybersecurity analysts. Sharma et al. (2024) used LIME and SHAP to explain the model's decisions when evaluating deep-learning based intrusion detection systems in IoT networks to explore the potential of explainable AI for this task. To show the importance of AI as a tool in security analysis and for making security models understandable, Sharma et al. (2024) leveraged explainable AI techniques for a deep-learning-based intrusion detection system in IoT networks, and used LIME and SHAP to facilitate the understanding of the model's judgement on predicting an intrusion. Pawlicki et al. (2024) analyzed the relationship between XAI and IDS and discussed some of the primary issues concerning transparency, trust and understandability of a human-made intrusion detection decision, which explainability would solve.

Automated incident response: Adaptive Cyber Defense.

One major change from finding threats to taking prompt and decisive action was the move from manual to automated incident response. Typical security operations included maintaining a roster of analysts for viewing alerts, evaluating their severity, identifying the appropriate countermeasures to take, and then manually following the response procedures. If these orgs received a lot of alerts within a period of time, these processes may cause issues. Alshamrani and Alshahrani (2023) proposed a multi-agent RL approach that achieves adaptive cyber defense and showed the efficacy of using multiple learning agents to deliver a set of suggestions during network defense decision-making in an evolving network context. They discovered that “adaptive defense” could be used to reduce the need for static defense policies as security mechanisms can take differing actions depending on the state of their environment.

Research on reinforcement learning also demonstrated that automated response mechanisms could acquire a defense policy as opposed to simply having response rules pre-

programmed and hard coded. Sewak et al. (2023) explained that deep reinforcement learning goes beyond classification and has potential in scenarios that might help with decision-making and suggest defensive choices in the complex cybersecurity context. For enhancing the training of autonomous cyber-defense agents in dynamic and adversarial environments, Farooq (2025) proposed a new concept of hybrid learning – a combination of reinforcement learning and supervised learning. The hybrid method addressed key challenges pertaining to learning stability, generalization and autonomous agents learning effective policies from experiences drawn from security related areas.

Also cited in the literature was the requirement for the adaptability as set response policies may not work if attackers change their tactics. Hu et al. (2020) derived that the adaptive defense could be formulated as a sequential decision-making process in which defensive responses were decided upon in the face of unknown attacks. Farooq (2025) announced that supervised learning can be fused with reinforcement learning so that the agents could use its learning to change its policy automatically. This research laid the foundations for automated response to go beyond orchestration of security and into the realm of real-time monitoring of the network, definition of what to do next to defend the network, and adapting the next set of actions to network feedback.

Adaptive Recovery, Resilience, and Autonomous Cyber Defense

Another major part of independent cyber defense was the concept of adaptation: what to do to get the systems back to normal after an attack had succeeded. Autonomous cyber defence would certainly have been incomplete without adaptive recovery, which centred on restoring attacked systems and getting back to normal following a successful defence. Being able to withstand, respond and recover from a cyber incident is also part of cyber-resilience – in terms of resilience to these cyber incidents has become an important

and core component of cyber-resilience research. Tzavara and Vassiliadis (2024) traced the history of cyber resilience and its progression from a security-centric perspective to a system or organization's ability to endure and bounce back from a disruptions caused by cyber events. The survey of case studies confirmed the complementary nature of the cyber-resilience measures in the cybersecurity management process, with the four types of measures pointed to by the case studies being: prevention, response, recovery, and continuous improvement of cyber-resilience capability.

The idea of adaptive recovery became significant as it becomes crucial to customize the response to a cyber incident based on its nature, scale and magnitude. Autonomous systems may be able to assess new conditions in a system and determine if a changed recovery mechanism is to be used; and static recovery procedures may be able to use predetermined recovery mechanisms to carry out a recovery program. Alshamrani and Alshahrani (2023) highlighted the significance of relying on the adaptive defense strategy selection in the multi-agent reinforcement learning framework, while Farooq (2025) correlated the concept of reinforcement learning and autonomous protection within adversarial environments.

The new literature was beginning to appear about autonomous cyber defense as an integrated defense capability that encompasses detection, decision making, response, adaptation and recovery. Autonomous agents had to make correct observations on the state of the network, make decisions about what to do and have the ability to adapt accordingly as attack conditions changed. I also looked at the recent trend of research into explainability and operating trust that was observed when AI took the decision to defend with virtually no human intervention. Sharma et al. (2024) pointed out that the notion of explainable AI (XAI) is vital for comprehending the decisions made in intrusion detection, and recovery was embedded in the broader context of cyber resilience by Z. Tzavara and D. Vassiliadis (2024).

Conceptual Framework Model

Intelligent Threat Detection (ITD), Automated Incident Response (AIR), and Adaptive Recovery (AR) were the independent variables included in the framework of this study and Autonomous Cyber Defense (ACD) was the dependent variable for this study. This architecture proposed that intelligent threat detection could better identify suspicious activity and newly evasive threats, automated response of incidents would allow

timely and appropriate responses to incidents, and adaptive recovery would assist in network recovery from cyber incidents and adapt the security mechanisms. The model then postulated that these three cyber security capabilities are all positively affected by the general autonomous cyber defense in dynamic network environments. The suggested relationships are $ITD \rightarrow ACD$, $AIR \rightarrow ACD$, and $AR \rightarrow ACD$ and correspond to H1, H2, and H3 respectively.

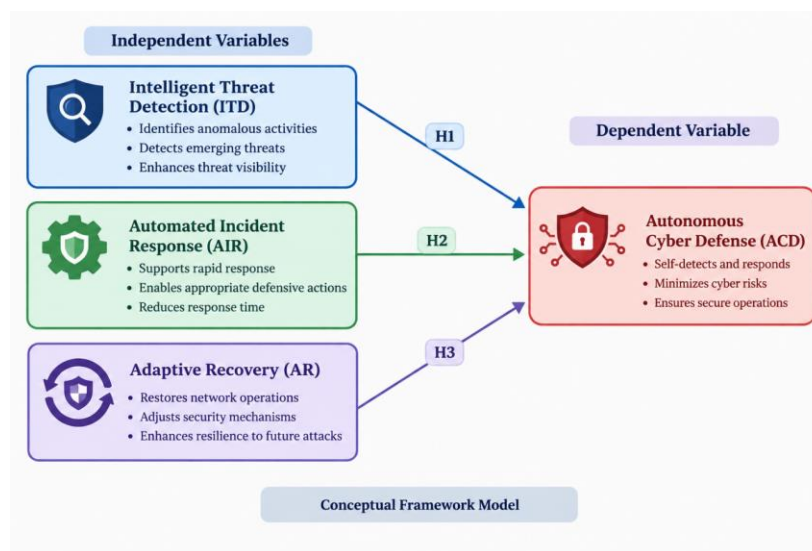


Figure 1. Conceptual Framework Model

Research Methodology

Research Design

This study used a quantitative, cross-sectional research design to study autonomous cyber defense in dynamic network environment. The design was chosen due to the focus of the study on the measurement of the relationships between Intelligent Threat Detection, Automated Incident Response, Adaptive Recovery, and Autonomous Cyber Defense based on numerical data in a structured form. The survey was designed to gather perceptions based upon a sample of cybersecurity and information technology practitioners with expertise in organizational network security, threat monitoring, incident response, and recovery.

Population and Sample

The target population was cyber security professionals, IT professionals, network or systems administrators, security analysts or information security practitioners using organisational information systems or network infrastructures. For the present study, a random sample of 300 respondents was drawn. The sample size was adequate to make descriptive and inferential statistical analysis treating the research variables and enabled the examination of the proposed relationships among the research variables. The respondents were selected using a purposive sampling technique since the participants should have relevant knowledge related to the

cybersecurity operations and network environment of the organizations.

Data Collection Procedure

Structured questionnaire was used to obtain primary data. The survey was sent to cybersecurity and IT professionals who met certain criteria by email. Questionnaire was sent electronically to eligible cybersecurity and IT professionals. Information about the aim of the study and the voluntary nature of participation was given before filling in the questionnaire. Principal components of the questionnaire were two major components. The first part gathered demographic and professional information such as: roles in the occupation and experience with cybersecurity. In the second section, the four study constructs were measured: Intelligent Threat Detection, Automated Incident Response, Adaptive Recovery and Autonomous Cyber Defense. The items were presented in a five point Likert scale, from strongly disagree (s.d) to strongly agree (s.a).

Data Analysis

Descriptive and inferential statistical method were used to analyze the data gathered. The numbers were then used to carry out descriptive statistics to obtain the mean and standard deviation of

Intelligent Threat Detection, Automated Incident Response, Adaptive Recovery and Autonomous Cyber Defense. These statistics give an overview of respondents' opinions of the four constructs. Using inferential analysis, the relationships between the independent variables and autonomous cyber defense were then investigated. Pearson correlation analysis was applied to ascertain the strength and direction of the relationship between the variables, and multiple linear regression analysis was used to investigate if Intelligent Threat Detection, Automated Incident Response and Adaptive Recovery were significant predictors of the outcome variable of Autonomous Cyber Defense. The regression analysis presented standardized beta coefficients (β), standard errors, t-values, levels of significance, R, R² and adjusted R². The test value of statistical significance was set as 0.05.

Results and Analysis

Descriptive Statistics

The responses from 300 cyber professionals and information technology practitioners were collated and analyzed to determine the overall status of Intelligent Threat Detection, Automated Incident Response, Adaptive Recovery, and Autonomous Cyber Defense.

Table 1.Descriptive Statistics of the Study Variables

Variable	N	Mean	Std. Deviation
Intelligent Threat Detection	300	3.87	0.71
Automated Incident Response	300	3.79	0.74
Adaptive Recovery	300	3.73	0.76
Autonomous Cyber Defense	300	3.84	0.70

Table 1 showed that Intelligent Threat Detection had the highest mean score of all the independent variables with a mean of 3.87 and a mean standard deviation of 0.71. The result showed that in general, the respondents noted that intelligent mechanisms that monitor the network, detect abnormalities and define potential threats are present. The small standard deviation indicated there was moderate consistency among responses.

A mean score slightly below four and a smaller stand deviation of 0.70, Autonomous Cyber Defense also attained a relatively high mean score, and participators generally had a positive perception of the autonomous cybersecurity capabilities within their organization. Automated Incident Response's mean was 3.79, and the standard deviation was 0.74. The responses found that the challenge of incident analysis,

prioritization and defensive action was generally accepted as facilitated by automated mechanisms. In terms of mean scores, Adaptive Recovery's score was the lowest at 3.73 SD 0.76, surpassing the middle of the five-point scale. The descriptive findings showed all four constructs with mean values exceeding 3.70, indicating in general positively assessed perceptions of AI-enhanced

cybersecurity abilities. The results also indicated that the top-rated average were threat detection, autonomous cyber defense, automated incident response and adaptation recovery. The standard deviations ranged between 0.70 and 0.76, which were relatively similar which did not show extreme dispersion of the responses.

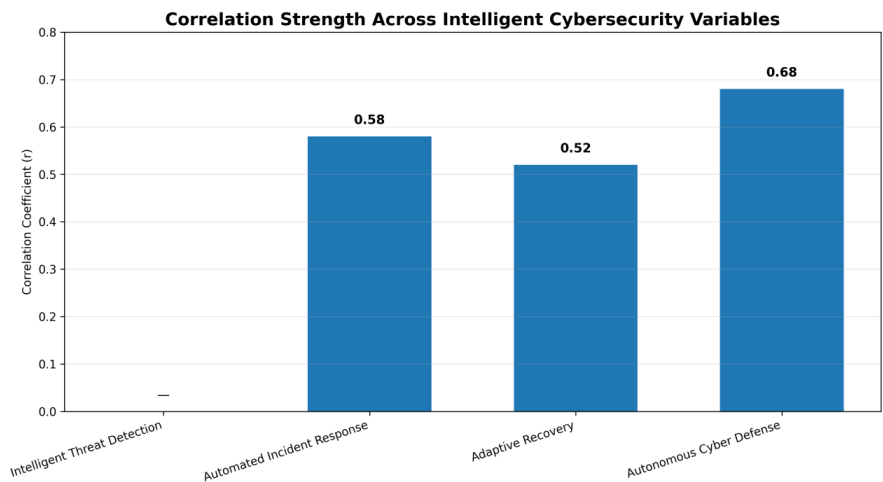


Figure 2.Descriptive Statistics of the Study Variables

Correlation Analysis

Pearson correlation analysis was performed to determine the direction and strength of the

relationships among Intelligent Threat Detection, Automated Incident Response, Adaptive Recovery, and Autonomous Cyber Defense.

Table 2. Pearson Correlation Matrix of the Study Variables

Variables	1	2	3	4
1. Intelligent Threat Detection	1			
2. Automated Incident Response	.58	1		
3. Adaptive Recovery	.52	.55	1	
4. Autonomous Cyber Defense	.68	.61	.57	1

Note. $p < .01$ (two-tailed). $N = 300$

All the study variables were shown to have positive and statistically significant relationships in the results shown in Table 2. The correlation between Intelligent Threat Detection and Autonomous Cyber Defense was found to be high with $r = .68$, $p < .01$. This was the highest correlation for the independent variable with the dependent variable. The findings showed than those who claimed to

have them more strongly tended to also claim to have autonomous cyber-defense capabilities. Additionally, there was a strong positive correlation of .61 ($p < .01$) between Bottomline Incidence Response automation and Autonomous Cyber Defense. This discovery suggested that the stronger automated response capabilities they disposed of, the greater degree of autonomous

cyber defense they exhibited. Adaptive Recovery produced a significant ($r = .57$, $p < .01$) positive correlation with Autonomous Cyber Defense, indicating a positive interrelationship between improvement/recovery and overall autonomous

cyber defense. The relationships between the independent variables were also positive, ranging from .52 to .58, such that the more robust the detection, the more robust the response/recovery.

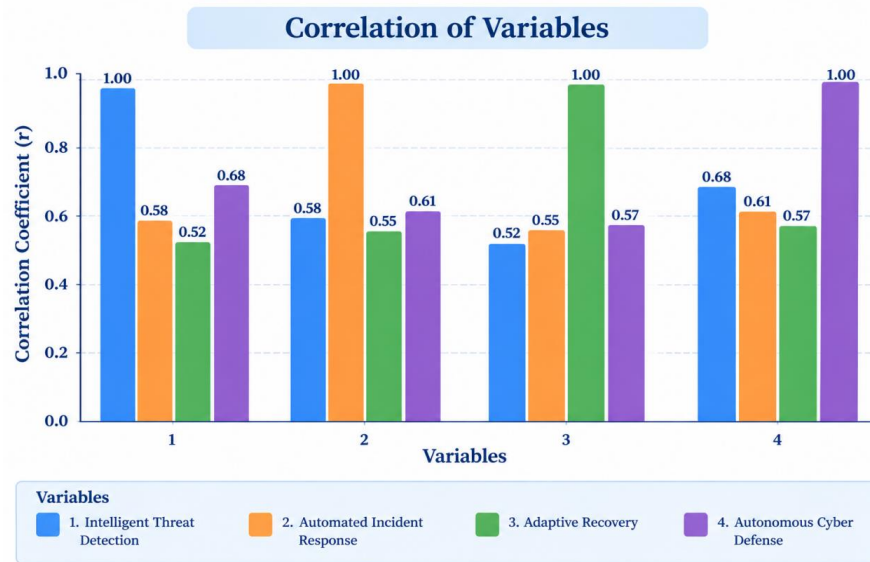


Figure 3. Pearson Correlation Matrix of the Study Variables

Multiple Regression Analysis

Table 3. Multiple Regression Analysis Predicting Autonomous Cyber Defense

Predictor	B	Std. Error	Beta (β)	t	p
Constant	0.721	0.184	—	3.92	<.001
Intelligent Threat Detection	0.421	0.047	.42	8.96	<.001
Automated Incident Response	0.312	0.049	.31	6.37	<.001
Adaptive Recovery	0.268	0.046	.27	5.83	<.001

Model statistics: $R = .764$, $R^2 = .584$, Adjusted $R^2 = .580$, $F(3, 296) = 138.48$, $p < .001$

The overall model was statistically significant as indicated by the regression results shown in Table 3, $F(3, 296) = 138.48$, $p < .001$. The overall fit of the model was sound with an overall R of .764 representing a strong relationship between the three predictors and Autonomous Cyber Defense. I.T.D., A.I.R., and A.R. accounted for 58.4% of the variance in A.C.D., based on the R^2 value of .584. The adjusted R^2 was .580, which indicates

that the explanatory power of the model was also high when adjusted for the number of predictors in it. The other 41.6 % of variance was due to other factors not modeled in the present study. The education factor of Intelligent Threat Detection proved to be a statistic positive predictor for Autonomous Cyber Defense ($\beta = .42$, $t = 8.96$, $p < .001$). The value for Automated Incident Response was a positive $\beta = .31$, $t = 6.37$,

$p < .001$. Adaptive Recovery also had a strong positive correlation with Autonomous Cyber Defense ($\beta = .27$, $t = 5.83$, $p < .001$). The three proposed relationships were supported statistically from the regression results. Of these predictors,

only Intelligent Threat Detection's β coefficient was more than .25, and its value was greater than all other predictors ($\beta = .42$), followed by Automated Incident Response ($\beta = .31$) and Adaptive Recovery ($\beta = .27$).

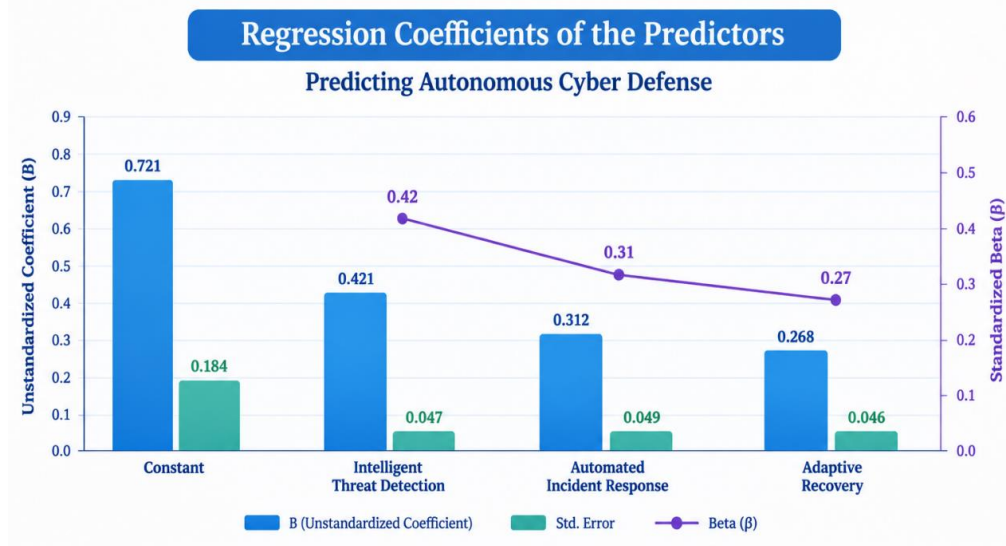


Figure 4. Multiple Regression Analysis Predicting Autonomous Cyber Defense

Hypothesis Testing

Table 4. Summary of Hypothesis Testing

Hypothesis	Relationship	β	p-value	Decision
H1	Intelligent Threat Detection $\rightarrow$ Autonomous Cyber Defense	.42	<.001	Supported
H2	Automated Incident Response $\rightarrow$ Autonomous Cyber Defense	.31	<.001	Supported
H3	Adaptive Recovery $\rightarrow$ Autonomous Cyber Defense	.27	<.001	Supported

H1 was supported by the results as Autonomous Cyber Defense had a strong positive correlation with Intelligent Threat Detection ($\beta = .42$, $p < .001$). The result showed that a high level of continuous identification of anomalous activities, continuous monitoring of network behaviour, and identification of potential threats were related to a high level of autonomous cyber-defence capability. The significance of the coefficient showed that the effect observed was not likely to be due to random variation among sample members. Further, both H2 and Automated Incident Response had positive coefficients that were statistically significant; H2 = .31, $p < .001$ and Automated

Incident Response = .13, $p < .001$. The findings indicated that the automatic processes of problem analysis and defensive reactions had a considerable impact on autonomous cyber defense processes. H3 was also in support, as the relationships between score on Autonomous Cyber Defense and Adaptive Recovery were significant and positive ($\beta = .27$, $p < .001$). This finding showed that the recovery mechanisms that enabled resuming services and adjusting to the conditions after an incident played a significant role in overall autonomous defence capability. A good amount of empirical evidence was found

with 58.4% of the dependent variable variance explained by the regression model.

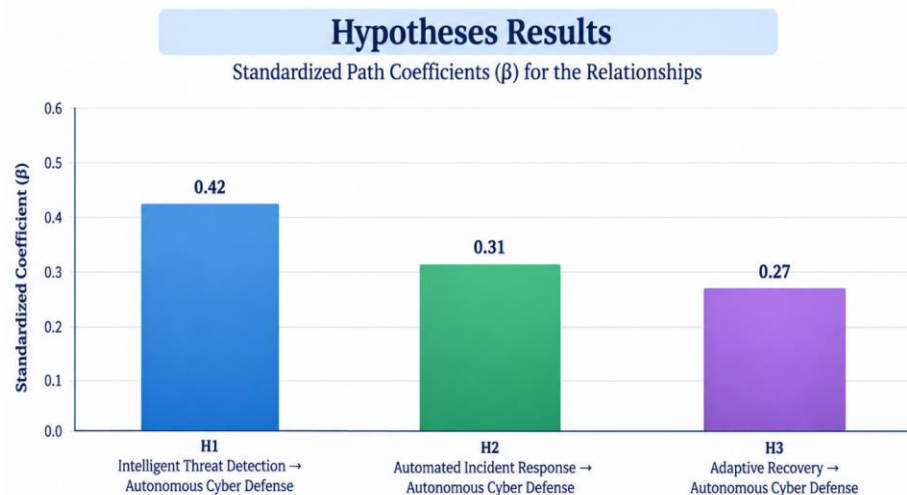


Figure 4. Summary of Hypothesis Testing

Discussion

The literature suggests that I.T.D. is a critical component linked to autonomous cyber defence: good autonomous capability necessitates long-term network observation via security systems alongside knowledge of network behaviours. They started using artificial intelligence, machine learning and deep learning algorithms to analyse huge security data sets to detect advanced and new threats. Recent studies have highlighted the importance of intelligent detection in enhancing cybersecurity, by utilizing anomaly recognition and adapting security systems on changing attack methods (Kaur et al., 2023; Salem et al., 2024). This view leads to the necessity to take a new approach to autonomous defense, one that differs from the current one, which is to describe security rules for the sensors to add static signatures. This vision inspired the concept of a defense system that doesn't rely on the same approach as before, such as scribing static signatures onto appliances associated with security rules defined on the sensor.

Automation plays a crucial role in cutting-edge Cyber Defense, and an automated Incident

Response is no exception. Existing methods of incident response would be tending to the incident using security analysts for triage, and for deciding what countermeasure to take in response to an alert – this is a problem when a lot of security incidents are being reported at the same time. The recent research of deep reinforcement learning (DRL) demonstrates the potential ability of the intelligent agent to learn defensive policies and make policy decisions based on the various cyber security scenarios (Sewak et al., 2023). Another important research area was the use of multi-agent reinforcement learning for improving decision making in coordinated cyber defense in dynamic networks, which was explored by Alshamrani and Alshahrani (2023). The following innovations made automation a tool that not only alerted on these events, but became the technology of intelligent action in cybersecurity defense.

Another important part of autonomous cyber security was how organizations could bounce back from a disruptive cyber incident – Adaptive Recovery. Research in Cyber-Resilience is beginning to integrate the security and ability to stand up, recover and quickly adapt to new threats

with ability to respond after disruption and ability to withstand disruption. Tzavara and Vassiliadis (2024) stressed the current status of cybersecurity and cyber resilience relation and the significance of recovery and adaptation element of organizational cyber resilience. Recent studies also emphasized the use of autonomous defense – requiring the security agent to adapt to changes in the environment – particularly in the context of learning-based methods (Farooq, 2025). The “adaptive recovery” enumerated in turn offers a more comprehensive perspective on cyber defense, in which the imperative to recover is a lifelong learning and adaptation cycle.

The literature also indicated that an autonomous cyber defence cannot be based solely on one function of any technology system, it should be based on multiple functions of the cyber defence. The elements of threat detection, incident response, and incident recovery were the sequential components of defense: threat detection information was used to inform the choices for subsequent stages in the process. Vyas et al. (2025) observed that intelligent cyber defense agents’ capabilities should be tested in real-world settings where they are not protected by other defenders, in the presence of different types of attacks. As in Loevenich et al. (2025), autonomous cyber defense, via deep reinforcement learning, large language models, knowledge graphs and cyber-threat intelligence, was discussed. Here, the study showed a progressive trend in adopting 'all-in-one' architectures that are focused on providing context- and adaptive-security whose decisions.

Flexibility, new knowledge (discovery), explainability and human supervision are crucial characteristics of autonomous cyber defense as observed in the new knowledge. AI systems offered quickly and automatically make decisions on security problems, but security practitioners lacked ways of comprehending and assessing automation decisions. Sharma et al. (2024) demonstrated the significance of XAI for grasping the decisions taken by intrusion-detectors, while Pawlicki et al. (2024) included explainability as one of the most important items in the radar screen when

leveraging AI to design intrusion-detectors. Autonomous cyber defense was more than "automated" defense, it was the "intelligent" counter-action that reacted to changes it sensed in its environment, adapted its defense, and allowed for resilient operations in the cyber domain.

Conclusion

The study showed that in the context of a "living network" – where the nature of attacks is continually evolving – the scope for autonomous cyber defense was increasingly growing into the facets of cyber security. By merging in the Intelligent Threat Detection, Automated Incident Response, and Adaptive Recovery, an autonomous defense capabilities model could be developed that encompasses everything. Intelligent Detection enabled threat identification in identification in a timely and effective manner; Adaptive Recovery bolstered network systems to recover quickly and adapt to evolving threat scenarios and conditions; and Automated Response enabled quick defensive response. The study emphasized the importance of integrating these capabilities into a cybersecurity system framework, and the continued need for the creation and implementation of explainable, adaptive, resilient and adequately supervised autonomous cyber-defense systems.

REFERENCES

- Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150. <https://doi.org/10.1002/ett.4150>
- Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189, 105124. <https://doi.org/10.1016/j.knosys.2019.105124>

- Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms—A comprehensive review. *Information Fusion*, 118, 102922. <https://doi.org/10.1016/j.inffus.2024.102922>
- Alshamrani, A. (2025). Federated hierarchical MARL for zero-shot cyber defense. *PLOS ONE*, 20(8), 111162. <https://doi.org/10.1371/journal.pone.0329969>
- Alshamrani, A., & Alshahrani, A. (2023). Adaptive cyber defense technique based on multiagent reinforcement learning strategies. *Intelligent Automation & Soft Computing*, 36(3), 2757–2771. <https://doi.org/10.32604/iasc.2023.032835>
- Farooq, M. O. (2025). Adaptive cyber defense through hybrid learning: From specialization to generalization. *Future Internet*, 17(10), 464. <https://doi.org/10.3390/fi17100464>
- Hu, Z., Zhu, M., & Liu, P. (2020). Adaptive cyber defense against multi-stage attacks using learning-based POMDP. *ACM Transactions on Privacy and Security*, 24(1), Article 6, 1–25. <https://doi.org/10.1145/3418897>
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Khan, M. A., Kim, J., & Kim, S. (2022). Deep learning for intrusion detection and security of Internet of Things (IoT): Current analysis, challenges, and possible solutions. *Security and Communication Networks*, 2022, 4016073. <https://doi.org/10.1155/2022/4016073>
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2, 20. <https://doi.org/10.1186/s42400-019-0038-7>
- Loevenich, J., Adler, E., Hürten, T., & Lopes, R. F. (2025). Design and evaluation of an autonomous cyber defence agent using DRL and an augmented LLM. *Computer Networks*, 262, 111162. <https://doi.org/10.1016/j.comnet.2025.111162>
- Morris, J. (2025). Evaluating reinforcement learning agents for autonomous cyber defence. *Applied AI Letters*, 6(3), e125. <https://doi.org/10.1002/ail2.125>
- Nguyen, T. T., & Reddi, V. J. (2023). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*, 34(8), 3779–3795. <https://doi.org/10.1109/TNNLS.2021.3121870>
- Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2024). The survey on the dual nature of xAI challenges in intrusion detection and their potential for AI innovation. *Artificial Intelligence Review*, 57, 330. <https://doi.org/10.1007/s10462-024-10972-3>
- Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (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>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7, 41. <https://doi.org/10.1186/s40537-020-00318-5>

Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, 25(2), 589–611. <https://doi.org/10.1007/s10796-022-10333-x>

Sharma, B., Sharma, L., Lal, C., & Roy, S. (2024). Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. *Expert Systems with Applications*, 238, 121751. <https://doi.org/10.1016/j.eswa.2023.121751>

Shi, Y., Zhang, H., Shi, L., & Xu, S. (2025). Autonomous cyber defense for AIoT using Graph Attention Network-enhanced reinforcement learning. *Computer Communications*, 241, 108265. <https://doi.org/10.1016/j.comcom.2025.108265>

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, 23, 1695–1719. <https://doi.org/10.1007/s10207-023-00811-x>

Vyas, S., Mavroudis, V., & Burnap, P. (2025). Towards the deployment of realistic autonomous cyber network defence: A systematic review. *ACM Computing Surveys*, 58(1). <https://doi.org/10.1145/3729213>

Zhou, Y., Liu, X., & Wang, Y. (2024). Consensus hybrid ensemble machine learning for intrusion detection with explainable AI. *Journal of Network and Computer Applications*, 235, 104091. <https://doi.org/10.1016/j.jnca.2024.104091>