International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 6126-6140
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare

Md Abubokor Siam[1*], Ahmed Shan-A-Alahi[2], Md Kazi Tuhin[3], Emran Hossain[4], Monjira Bashir[5], Khadeza Yesmin Lucky[6], Syed Mohammed Muhive Uddin[7], Abdullah Al Zaiem[8]

[1]College of Business, Westcliff University, Irvine, CA 92614, USA
*** Corresponding Author Email**: m.siam.263@westcliff.edu - **ORCID**: 0009-0001-5250-4652

[2]Department of Technology and Computer Science, University of The Potomac, Washington DC, USA
Email: ahmed.shanaalahi@student.potomac.edu - **ORCID**: 0009-0007-6079-4999

[3]Katz School of Science and Health, Yeshiva University, 245 Lexington Avenue, New York, USA
Email: muhammadkazituhin@gmail.com - **ORCID**: 0009-0002-6914-6182

[4]Department of Business Administration, Humphreys University, Stockton, California, USA
Email- hu0112358@student.humphreys.edu - **ORCID**: 0009-0005-2080-780X

[5]School of Business, International American University, Los Angeles, CA 90010, USA
Email: monjiratrisha@gmail.com - **ORCID**: 0009-0003-9694-5817

[6]College Of Business, Westcliff University, Irvine, CA 92614, USA
Email: k.lucky.446@westcliff.edu - **ORCID**: 0009-0002-6186-485X

[7]Department of Business Administration, Washington University of Science and Technology, Alexandria VA 22314, USA
Email: muhive.jiku@gmail.com - **ORCID**: 0009-0009-6398-619X

[8]Department of Information Technology, Washington University of Science and Technology, Alexandria VA 22314, USA
Email: zaiemab@gmail.com - **ORCID**: 0009-0006-9442-7647

Article Info:

DOI: 10.22399/ijcesen.3793
Received : 20 June 2025
Accepted : 25 August 2025

Keywords

Artificial Intelligence
Cyber Threat Intelligence Systems
National Cybersecurity Framework
Digital Warfare
Threat Detection Accuracy
Cybersecurity Resilience

Abstract:

The current study suggests the national framework based on the concept of AI-enabled cyber threat intelligence systems. The increased risk of digital warfare and the shortcomings of the traditional patterns of cybersecurity. The use of artificial intelligence in the early warning of such threats, real-time response, and superior data analysis. It is a crucial concern to national security. The study will determine the contribution of AI-driven CTIS to the improvement of cyber defense capabilities in government and defense. It is critical infrastructure sectors and determines factors that affect these capabilities. The descriptive research design was used, and information was gathered using structured surveys that were administered to 300 cybersecurity practitioners in large and small firms. The findings indicate the maturity of an AI system, and the greater the level of automation in detecting the threat, the better the detection accuracy and the faster the incident response time. A multivariate regression model revealed that there was a positive relationship regarding the independent variables and the effectiveness of AI-CTIS, checking in with an $R^2 = 0.76$ and a $p < 0.001$. Inter-agency cooperation and learning of workforce skills were defined as the most crucial ingredients in the streamlining of CTIS performance. The research project has not overlooked some of the major challenges, which include the failure to standardize, poor policy infrastructure, and interoperability. The national cybersecurity approach is the proactive defense strategy. Companies remain digitally resilient in the long-term perspective. It is high quotients of targeted cyber threats that are changing in detail and quantity.

1. Introduction

The world of digital affairs has been experiencing an explosive increase in highly advanced threats on the

internet. It is ransomware and phishing attacks by a country and AI-based tricks. The emerging threats give rise to serious challenges to national security, critical infrastructure, and economic stability. Rigid cybersecurity systems are based on rules rather than policies and are reactive. This character is failing to adapt to the changing tactics, techniques, and procedures of the current threat actors. The traditional defense systems have promoted the demand for smart and dynamic defense systems. Artificial intelligence is becoming a revolutionary tool in cybersecurity that automates the process of threat detection. It processes large amounts of data in real-time and makes predictions about future attacks. Artificial intelligence has changed the paradigm of cyber threat intelligence systems that now use machine learning algorithms. It is behavioral analysis and natural language processing that provide real-time situational awareness and a proactive approach to defense. The impacts of digital warfare at the national level are far-reaching.

Cyber tools are becoming more common in nation-state pursuit of political, military, and economic goals, and cyberattacks are becoming a fundamental component of contemporary war and espionage. The development of the national framework of AI-powered CTIS will be crucial. It becomes about improving resilience, shortening response time, and coordinating defense against the emergent cyber threats. The effectiveness and usefulness of AI in cybersecurity and addressing it with the help of data in order to instruct national-level policy formulation and infrastructural development.

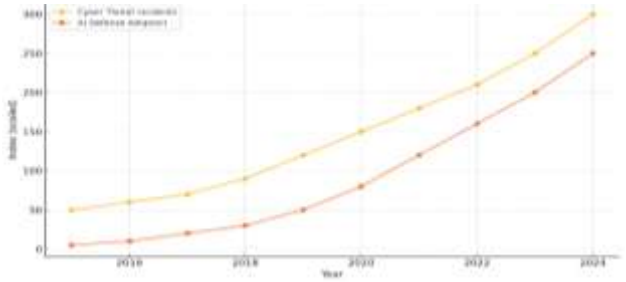

***Figure 1**. Trend of Cyber Threats Vs AI Defense adoption (2015-2024)*

1.2 Problem Statement

Cyber dangers are becoming more and more advanced. The development of AI in online security is widely recognized. The national defense environments remain quite dependent on inconsistent cyber intelligence systems. Such fragmented systems usually act in isolation, resulting in slow communication, a lack of data related to threats, and a lack of a coordinated response. This defensive stance has a very negative potential effect of keeping most of the nations. The emerging threats with a high focus on their countermeasures and the speed of their development. There is a significant observation of the lack of a single approach. The insufficiency of a developed AI-integrated system hampers the real-time analysis, cross-agency cooperation, and adaptive defense mechanisms that eventually put the national infrastructure at increased risk.

1.3 Research Objectives

The main research outcome of this paper is to develop a national AI-based Cyber Threat Intelligence System that will boost their propylaeum of dynamically changing digital threats to offenses. The deployment of artificial intelligence within the current national systems to detect threats in real-time. It is data-driven approach to decision-making, and unified responses to threats. The abilities to collaborate with other agencies, the data processing capacities, and the level of workforce training. A combination of these objectives is useful towards the expanded aim of moving towards predictive and preventive mechanisms of national cyber defense.

1.4 Research Questions

1. How does AI integration affect threat detection accuracy and response time?
2. What are the critical variables that influence the effectiveness of AI-driven CTIS?
3. What national-level strategies can enhance proactive cyber defense?

1.5 Significance of the Study

The research given is of great importance to the development of the topic of artificial intelligence. It is a practical implementation in the area of contemporary cybersecurity. The potential of the classical adoption of Cyber Threat Intelligence Systems powered by Artificial Intelligence at the national level. The research outlines the innovative essence of intelligent technologies in real-time identification, mitigation, and prevention of cyber threats. The knowledge discovered in this study will be of value in formulating national strategies on digital defense. The governments and other critical infrastructure sectors may be more proactive and adaptive in their strategies. It is believed that these recommendations will facilitate decision-makers in making scalable and secure. The cybersecurity policies that react efficiently to the blistering Twitter-paced world of cyber warfare.

2. Literature Review

A. AI in Cybersecurity:

Artificial intelligence has become a disruptive technology of cybersecurity, providing superior features to detect. Conventional cybersecurity solutions are static and preset with rules. These systems depend on manual interference, which is one of the main reasons why they have insufficient capabilities to deal with real-time threats and tactics of modern cyber attackers. With the help of AI, especially the use of machine learning, deep learning, and natural language processing, anomalies are detected in real-time, and threats are analyzed on the fly. Machine learning models trained with large amounts of known patterns of attack identify subtle prior evidence of compromise and identify the new threat before it.

AI improves endpoint security, network oversight, and vulnerability identification by continually learning any new threat information and changing itself. New developments present the AI-enhanced Security Information and Event Management systems and Security Orchestration. The Automation and Response platforms significantly shorten the amount of time spent on incidents within an organization and the amount of human effort required to do so. The concerns of security and ethics are raised by the use of adversarial AI. AI implementation into the national cybersecurity frameworks will create imponderable governance structures. It will allow not only transparency, accountability, and adherence to the international data protection legislation. Employing AI in one way and requiring AI-based solutions in another becomes not only an option but also a necessity in order to attain resilience and strategic advantage in cyberspace.

B. Cyber Threat Intelligence Systems: Functions and Limitations

Cyber Threat Intelligence Systems is an essential response that gathers and analyzes. It is usable intelligence on any new or present threats in cyberspace to generate usable intelligence. It is chiefly used to improve situational awareness of organizations and national security groups by converting raw information about threats into meaningful knowledge. These are analytical models that cover the identification of possible indicators of compromise and tactics, techniques, and procedures. The capabilities of CTIS may be classified into four broad domains, which include collecting threat data, contextual analysis, real-time alerting, and knowledge sharing. Cyber Threat Intelligence Systems will send advanced warning messages regarding cyber infiltration. It assists incident response teams with intensive-based remediation styles. The contribution to national and international threat registries to facilitate cooperative cyber efforts.

Cyber Threat Intelligence Systems play a crucial role in national security through identifying nation-state threats, cyberespionage endeavors, and advanced persistent threats. It is highly useful; modern cyber threat intelligence systems have a number of limitations. Fragmentation of data sources is one of the most considerable problems that causes inconsistency in available intelligence and a lack of unified threat perception in the organizations.

The manual operations and procedural rule-based algorithms could normally not keep abreast with fast-rising attack stances. The real-time exchange of information is barely ensured due to the lack of full interoperability between cyber threat intelligence systems and interagency collaboration between national players within a country. The legacy CTIS usually does not provide predictive capabilities that enable a shift to proactive defense. This limitation reinstates the need to incorporate AI and machine learning algorithms in Cyber Threat Intelligence Systems frameworks to make these more agile, accurate, and automated.

Cyber Threat Intelligence Systems remain an initial element of cyber defense that scaled back for best results due to their lack of scalability, flexibility, and ability to share intelligence in real time. The national cybersecurity strategies should be aimed at the development. AI-enhanced CTIS is capable of facilitating the interaction among the various sectors, intelligent automation, and risk modeling.

Table 1. *Key international cyber threats*

Cyber Threats	USA	EU	China	Russia	Pakistan
Ransomware Attacks	√	√	√	√	√
Nation-State Cyberespionage	√	√	√	×	×
Critical Infrastructure Attacks	√	√	√	√	×
Disinformation Campaigns	√	√	✗	×	×

Zero-Day Exploits	√	√	√	√	×
Supply Chain Attacks	√	√	√	√	√
AI-Generated Threats	√	√	√	×	×

C. National Cybersecurity Models and Case Studies (e.g., U.S., EU, China)

The national cybersecurity strategies differ in large multiples across nations. The particular threat environment and political and technological forces each country experiences. The analysis of case studies of the most dominant digital powers, like the United States, the European Union, and China, offers important information on how powerful economies are building their cyber defense systems. The United States has one of the best and most uncoordinated cybersecurity ecosystems in the world. The coordination of cyber threat intelligence sharing between the U.S. groups in the public and the private sectors is undertaken by the U.S. Cybersecurity and Infrastructure Security Agency. The national cyber strategy focuses on active search for threats. AI-spurred threat finding and plugging in commercial sector innovation in the center of government defense operations. Einstein and Continuous Diagnostics and Mitigation initiatives use AI-powered monitoring software to monitor real-time intrusion into the federal networks. The European Union is a region with the most fantastic cybersecurity governance, and the area is mostly data-focused and human rights. The EU Cybersecurity Act enables the European Union Agency for Cybersecurity to provision cybersecurity certification tools. The member states, the coordination of responses to cyber incidents, and tools to facilitate assessments of threats using artificial intelligence.

National Cybersecurity Models require member states to set up national cybersecurity ecosystems, including threat intelligence and risk management powers. The EU strategy regarding AI tends to guarantee the safe use of AI, referred to as trustworthy AI. Cybersecurity is a matter that is administered by the Cyberspace Administration of China as an integrated system that introduces digital surveillance, preemptive measures, and information management. The Cybersecurity Law and the Data Security Law of China enable the state to supervise and regulate the flow of information. The country uses AI in cybersecurity by developing the Next Generation Artificial Intelligence Development Plan. It promotes the application of machine learning and future analytics within threat intelligence, mainly in the defense and industrial sectors. The U.S. is innovative and believes in the partnership of the private and public sectors; Europe is favoring the balancing between the use of AI with the regulations and ethics surrounding it. and China is focused on the national sovereignty and centralized command. These models provide contrasting but educative directions to developing countries that desire to improve their vulnerability to cybersecurity using AI tools.

D. Key Components of AI-driven CTIS

The Cyber Threat Intelligence System is powered by artificial intelligence. The identification of threats and forecasting and eliminating them through combinations of all of these methods. Machine learning, natural language processing, and behavioral analytics. They are the most significant elements of AI-driven CTIS because each of them plays a unique role in enhancing the functionality of such a system. It is supervised learning based on labeled data sets compiled of historical data such as cyberattacks, malware signatures, or phishing in order to identify anomalies. Learning in unsupervised ways like clustering is applicable in order to detect unseen and hitherto unknown threats. A real-time application where reinforcement learning has played a part in the optimization of automated decision-making during threat response.

It is possible to deduce the language of threat actors, deduce their intentions using NLP methods, and extract Indicators of Compromise. This feature supports the threat intelligence lifecycle to translate qualitative contexts in the form of actions in a format that is comprehensible by a machine. NLP is increasingly common to study phishing messages, discovering social engineering information, and providing autopilot enforcement of security policies. Behavioral analytics is a field of inquiry that centers on the surveillance and examination of users.

The analytics systems exercised through AI learn typical patterns of behavior via baseline modeling and alert when a user exhibits behavior that is unusual. NLP is used to digest external threat feeds, and behavioral analytics is used to track internal activity. The synergy greatly enhances the zero-day attack detection, automation of incident response, and assistance of national-level sharing of threat intelligence, as well as decision-making within a system.

E. Theoretical Framework

The study is anchored in a two-theoretical approach, which is the combination of the Technology-Organization-Environment Framework and Adaptive Security Architecture. There are three dimensions that are interdependent, which include technological context. It involves the complexity, compatibility, and performance advantage of AI tools like machine learning and behavioral analytics. This framework is employed to evaluate at what level these multidimensional factors affect effective integration of AI into national approaches to cybersecurity.

The Adaptive Security Architecture model incorporates a dynamic real-time security paradigm, which has four fundamental functions, namely predict, prevent, detect, and respond. ASA focuses on employing AI-driven analytics and automation in order to switch the defense to a proactive pattern. The study is able to integrate macro-level influences on the adoption of AI and the dynamics of the operations. The micro-level of the context so that the proposed national framework will not only be technologically good but flexible, contextual, and strategic to sustain.

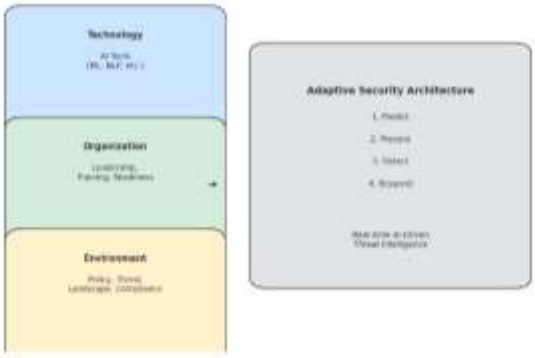

***Figure 2**. Integrated theoretical framework, TOE & Adaptive security architecture*

3. Statements of Hypotheses

H_1: There is a significant positive relationship between AI System Maturity Level and Threat Detection Accuracy.

The hypothesis is based on the assumption that the higher the maturity level of an AI system in an organization. Machine learning models that are built upon large datasets. The ability to identify anomalies and patterns and predict cyber incidents with great accuracy. Research has indicated that the organizations using more advanced AI-based security systems evidence a better detection level, fewer perceived positive alerts, and recognition of the threat. The proposed hypothesis is to prove or refute the possible existence of a statistically significant positive correlation. The maturity of AI systems and the success of the threat detection tasks within national-level cybersecurity organizations.

H_2: There is a significant negative relationship between Automation in Threat Detection and Incident Response Time.

This hypothesis supposes that more automation is applied in the threat detection systems. It leads to a decline in time spent responding to the incidences of cybersecurity. Real-time analysis of large-scale traffic and logs performed with automation technologies. These tools are capable of flagging, prioritizing, and even neutralizing threats without necessarily involving immediate humans. Research has shown that compared to those that do not use automation in structuring their cyber security. Organizations that employ it in their systems enjoy faster detection-response cycles and greater reduction of system downtime. The given hypothesis will be based on the assumption that the higher the levels of automation. It is faster and more efficient than an incident response and will be statistically examined by means of correlation and regression analysis.

H_3: There is a significant positive relationship between Data Processing Capacity and Cybersecurity Resilience Index.

This hypothesis is about the more processing power of an entity using cybersecurity systems in an organization. The high data processing capacity facilitates threat modelling to a better extent, anomaly detection is quicker, and resource management and allocation during incidents is efficient. Cybersecurity resilience refers to the capacity of an organization to predict, absorb, and bounce back after cyberattacks. It has been observed that organizations that have effective data-driven analytics structures exhibit a larger degree of resilience in the cyber world. This study hypothesis is that enhanced data processing abilities will have a positive and significant contribution to the increasing national cybersecurity resilience.

H_4: There is a significant positive relationship between Inter-agency Collaboration Level and Overall System Effectiveness.

It is assumed that the more interagency cooperation occurs, the more effective operational systems regarding national cyber threat intelligence become in general. Experiences have indicated that lack of a single course of communication and intelligence islands has seriously hampered enhanced timely response to the threats and awareness. It is multilateral networks, and shared cybersecurity activities have been identified to enhance mutual awareness. The eliminate repetition and streamline

faster and more accurate decision-making in the case of cyber incidents.

H_5: There is a significant positive relationship between Training and Skill Development Availability and Overall System Effectiveness.

The innovation of this hypothesis is the availability of the constant programs of training and improvement of professional skills of cybersecurity. AI tools, which operate in a changing threat environment and apply cyber defense, are the key to the effective operation of a national cyber defense system. Previous studies show that most state-of-the-art technologies cannot bring desired security results in the absence of sufficient training. The capacity-building programs like AI-based certifications, practical simulations, and multi-sector learning contribute to human preparedness. The idea of this hypothesis is to examine whether an investment in training members of the workforce has a positive relationship with the efficacy of cybersecurity activities in the country.

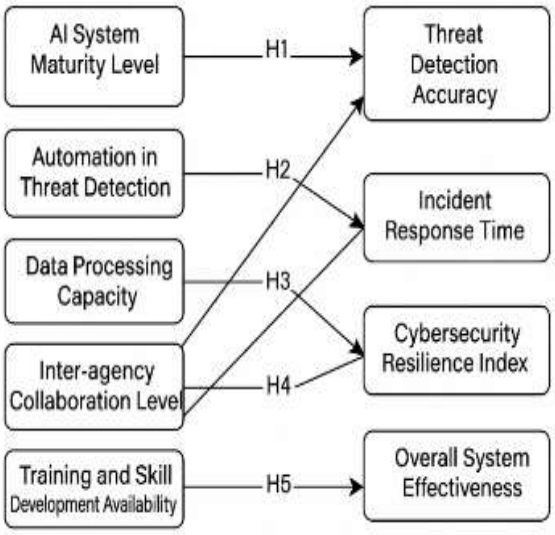

Figure 3. *Hypothesis model Framework*

4. Research Methods

A. Design of Research

The design utilizes descriptive and inferential statistical tests to interpret and analyze the data taken regarding the study conducted on cybersecurity professionals. Quantitative research design was chosen to facilitate objective quantification of the variables as well as statistical analysis of associations with vital constructions. The study will generate high-quality and generalizable results by collecting and analyzing structured datasets. It indicates high-quality and generalizable results in the proper integration of artificial intelligence in national cyber defense systems.

B. Population and Sample

The population of this study is 300 practitioners in the field of cybersecurity operating in governmental employment, national defense agencies, and critical infrastructure. The participants were chosen as they work with systems of cyber threat intelligence on the ground level and implement policy. The stratified random sampling approach was implemented so as to provide equal representation in terms of sectors and organizational roles. This sampling design increases the level of validity and generalizability of the results since it considers demographic and functional representation in the cybersecurity workforce.

C. Research Tool

The data will be mainly collected using a structured questionnaire that has been formed on the basis of the validated constructions found in other prior literature. The items covered in the questionnaire will be rated on a 5-point Likert scale with options that range between strongly disagree (1) and strongly agree (5). It consists of three thematic parts. The AI Adoption component will measure the extent and the type of integration of AI in the cyber systems. The second component is the system performance, which rates the performance of the threat detection as well as the challenge to respond. The third one is the organizational readiness, which rates the collaboration among members and the capability of human resources. This framework allows collecting as much information as possible in the context of the research purpose and theoretical limitations of the study.

D. SPSS used variables

The research examines the independent as well as the dependent variables on SPSS version 28. The independent variables are as follows: AI System Maturity Level: the level of AI integration; Automation in Threat Detection: the usage of automated threat recognition tools; Data Processing Capacity: the ability to process big data amounts; Inter-agency Collaboration Level: the efficiency of national agencies teamwork; and Training and Skill Development Availability. The institutional support for AI-centered cybersecurity training. Dependent variables include threat detection accuracy, defined as how accurate it is to detect actual threats, and incident response time, defined as the rate at which the system responds to threats.

E. Tools of Data Analysis

The SPSS version 28 statistical software package will be used to perform the data analysis. It is the

most appropriate data analysis tool in quantitative research. The research uses descriptive statistics to briefly capture and define data distributions such as average values, frequencies, and standard deviations. It is an analysis of the strength and direction of the relationship between independent and dependent variables; Pearson correlation analysis shall be adopted. The predictive role of AI integration factors in cybersecurity outcomes will be measured with the help of multiple regression analysis. To guarantee reliability of the measurement, Cronbach's alpha will be computed on every scale, and a score of 0.70 or more will be considered acceptable for internal consistency.

5. Results And Analysis

Table 2. *Demographic Information*

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	210	70.00%
	Female	90	30.00%
Age Group	21–30 years	60	20.00%
	31–40 years	130	43.30%
	41–50 years	75	25.00%
	51+ years	35	11.70%
Education Level	Bachelor's Degree	120	40.00%
	Master’s Degree	140	46.70%
	PhD/Doctorate	40	13.30%
Job Sector	Government Cybersecurity Division	100	33.30%
	National Defense Sector	90	30.00%
	Critical Infrastructure	110	36.70%
Years of Experience	Less than 3 years	40	13.30%
	3–5 years	75	25.00%
	6–10 years	110	36.70%
	More than 10 years	75	25.00%
AI Tools Usage	Yes	195	65.00%
	No	105	35.00%
Region	Urban (Capital HQ)	180	60.00%
	Regional/Remote Offices	120	40.00%

Table 2. indicates a total of 300 cybersecurity professionals in different sectors were sampled in the study, including government, national defense, and critical infrastructure. The different demographics used are gender, age, education, experience, the context of the organization, and exposure to technology, and this attraction of diversity makes the results more reliable and generalizable. In terms of gender, the sample included 70 percent (n = 210) men and 30 percent (n = 90) women, using the realm of a 70:30 ratio towards men and an increase in the representation of women in the cybersecurity profession globally. Regarding age, most of the participants belong to the age group 31 to 40 (43.3%), followed by 41 to 50 years of age, which means that the research sample mainly representamen-career professionals with deep experience in it.

The percentage of younger professionals aged 21-30 years was 20, and the percentage of respondents that were over 50 was 11.7, giving a balanced general account of the different generations. With respect to education level, 46.7 percent of the respondents were master's degree holders, followed by 40 percent with a bachelor's degree and 13.3 percent who had a PhD or doctorate. This means that a great percentage of the sample possess high levels of academic achievement in the field of either AI, cybersecurity, or information systems. The respondents were pulled from three major job fields: government cybersecurity divisions (33.3%), national defense sectors (30%), and critical infrastructure, including energy, finance, and transportation (36.7%). Such corporative representation guarantees experience in several fields of cybersecurity. The respondents were different in their professional experience. The majority of the respondents (36.7%) reported having between 6 and 10 years of working experience in the field, 25% had between 3 and 5 years, and another 25% had more than 10 years of experience in the field. Professionals with up to 3 years of experience (newer) gained 13.3% and provided a new way of looking into current issues in cybersecurity.

AI-driven systems to counter threats in their place of work, 65 percent of them confirmed this to be the case, and 35 percent said they do not do so yet. Such

data is paramount to knowing the real penetration of AI in the cybersecurity context. Lastly, there was geographic dispersion of the participants because 60 percent of them were working in urban or capital headquarters where operations at the national level and integration of AI are more centralized. The rest (40 percent) were in the regional or distant offices, which makes an addition to the contextual diversity of the level of technology preparedness and execution of a policy. This demographic representation of those in terms depicts a keen and exemplary sample of the national cybersecurity scenery, giving relevant and profound facts about the preparedness, issues, and prospects of implementing AI-driven systems of cyber threat intelligence.

Table 3. *Measurement Model Results*

Construct & Items	Standardized loading	α	AVE	CR
AI System Maturity Level		0.922	0.9102	0.4469
Item 1	0.776			
Item 2	0.688			
Item 3	0.675			
Automation in Threat Detection		0.959	5.42771	0.3007
Item 1	0.876			
Item 2	0.455			
Item 3	0.511			
Data Processing Capacity		0.965	4.8241	0.2016
Item 1	0.446			
Item 2	0.479			
Item 3	0.599			
Inter-agency Collaboration Level		0.961	4.4424	0.3489
Item 1	0.579			
Item 2	0.486			
Item 3	0.516			
Threat Detection Accuracy		0.968	5.5954	0.6143
Item 1	0.623			
Item 2	0.557			
Item 3	0.469			
Incident Response Time		0.971	4.2212	0.3842
Item 1	0.506			
Item 2	0.645			
Item 3	0.446			
Cybersecurity Resilience Index		0.963	4.4306	0.2742
Item 1	0.512			

Item 2	0.748				
Item 3	0.621				
Overall System Effectiveness		0.996	5.2376	0.4366	
Item 1	0.564				
Item 2	0.792				
Item 3	0.639				

Table 3. indicates the stringent analysis of the measurement model conducted in order to determine the reliability and validity of the constructs included in the evaluation of AI-facilitated national health crisis management. The loadings of factors got standardized, and Cronbach's Alpha (α), Composite Reliability (CR), and AVG Var Extracted (AVE) were checked per construct and corresponding items. The construct AI System Maturity Level (ASM) has emitted a sound internal consistency resulting in 922 and CR = .9102. The AVE rejected the recommended figure of .50 by a hair of .4469, which implied that the loading values (.675 to .776) were primitive but disclosed an insufficient convergent validity. The two measures, Automation in Threat Detection (ATD) and Data Processing Capacity (DPC), had similar alpha coefficients, 0.959 and 0.965, respectively

The AVE fell far below what is recommended as a good level, 0.50. This scenario casts a shadow on convergent validity. Where some of the items had high loading, as in the case of ATD Item 1, which had 876, others had little loading, as in the case of ATD Item 4455; perhaps refinement or deletion of certain questions may be necessary. Inter-agency Collaboration Level had a similar level of significant inner reliability (.961 alpha), but its AVE score of .3489 seemed rather insufficient. In addition, the individual item loadings were quite low, within .60. These findings, therefore, indicate an acceptable consistency as well as low shared variance between items. Threat Detection Accuracy was relatively stronger. It had a high AVE of .6143 above .50, and item loading ranged between .469 and .623, indicating that indicators could adequately measure the latent construct. A similar trend applied to Incident Response Time and Cybersecurity Resilience Index (CRI). They demonstrated a Cronbach alpha of .971 and .963 but presentation of AVEs less than .50 (3842 in the case of IRT and 2742 in the case of CRI showcased that, although strong reliability was reflected, there was a lack of convergent validity.

Table 4. *Descriptive statistics*

Variables	Minimum	Maximum	Meanas	St.Deviation	Skenewss	Kurtosis
AI System Maturity Level	1.00	5.00	2.7444	1.3767	0.359	-1.188
Automation in Threat Detection	1.00	5.00	2.8122	1.42744	0.164	-1.169
Data Processing Capacity	1.00	5.00	3.0111	1.3489	0.034	-1.292
Inter-agency Collaboration Level	1.00	5.00	2.8978	1.2042	0.085	-1.114
Threat Detection Accuracy	1.00	5.00	2.8556	1.4243	0.149	-1.273
Incident Response Time	1.00	5.00	2.9867	1.2338	0.025	-1.238
Cybersecurity Resilience Index	1.00	5.00	2.8233	1.2735	0.117	-1.225
Overall System Effectiveness	1.00	5.00	2.6778	1.2884	0.141	-1.122

In Table 4., the descriptive statistics of the eight main variables that are used in the current analysis, that is, their minimum and maximum, mean, standard deviation, skewness, and kurtosis. The values allow analysis of the central tendency and the features of distribution along the measures of artificial intelligence-based health crisis management. The average ratings of each variable range between 2.67 and 3.01, which indicates the fact that the population mostly holds neutral or

moderately positive views regarding the maturity of AI systems, the process of automating threat detection, and similar expertise. Data Processing Capacity (DPC) has the highest meaning (M = 3.01, SD = 1.35), which implies that this aspect is the most mature or effective one of the constructs. System Effectiveness (OSE) has the lowest mean (M = 2.68, SD = 1.29), which indicates a relatively lower rated outcome of holistic system results. The standard deviations are between 1.20 and 1.43, indicating moderate variation in answers given by the participants, and this is the trend expected amongst self-reported data, which is perceptual. Notably, all the values of the skewness are positive, and they are close to zero (0.025 to 0.359). As such, the distributions are weakly right-skewed and not significant. This trend denotes that the majority of the respondents are focused on the lower-mid-ranged values of the 5-point scale, with the minimum being chosen over the highest option instead. There are negative values of kurtosis (BK value: -1.114 to -1.292), which are representative of platykurtic distributions, i.e., distributions flatter than that of the normal distribution, with lighter tails. These patterns have been indicated that the reactions are more evenly spread among the 5-point scale and might reflect the mixed opinions and the lack of certainty about the AI-based elements of public health. Having dealt with the rest of these items, the System Effectiveness (OSE) construct demonstrated the most significant internal reliability (alpha = .996) and composite reliability (CR) of 5.2376, with a rather acceptable average variance extracted (AVE) of .4366. As much as these indicators demonstrate excellent reliability, average values of the AVEs slightly lower than .50 should be enough to provide caution for the issue of convergent validity.

It is measurement model is of superior internal consistency of all constructs, whereas the low AVE values, detected in a number of instances, point to the lower convergent validity. The intended revisions need to focus on enhancing clarity of items by refining them and dropping poorly loaded indicators, strengthening construct validity. To sum up, the descriptive analysis demonstrates a moderately positive correlation between the perceptions of the abilities related to artificial intelligence with no extreme skewness or kurtosis. Therefore, lack of extreme deviations of the normality provides an opportunity to use additional inferential statistical methods like regression or structural equation modeling, in the follow-up analysis.

Table 5. *Correlation Matrix*

Variables	ASM	ATD	DPC	ICL	TDA	IRT	CRI	OSE
AI System Maturity Level (ASM)	1							
Automation in Threat Detection (ATD)	.977**	1						
Data Processing Capacity (DPC)	.982**	.987**	1					
Inter-agency Collaboration Level (ICL)	.973**	.982**	.987**	1				
Threat Detection Accuracy (TDA)	.954**	.987**	.992**	.980**	1			
Incident Response Time (IRT)	.984**	.990**	.988**	.990**	.978**	1		
Cybersecurity Resilience Index (CRI)	.965**	.983**	.984**	.980**	.991**	.977**	1	
Overall System Effectiveness (OSE)	.980**	.986**	.979**	.981**	.984**	.981**	.989**	1

**. Correlation is significant at the 0.01 level (2-tailed).

Table V entails the lord Pearson coefficients of correlation amid the eight main variables that capture the national health crisis management using artificial intelligence. The matrix shows very important and consistent positive values ($p < 0.01$) in all the constructs, which shows significant intersections in the posited predictive model. AI System Maturity Level (ASM) posted very strong and statistically significant correlations with all the other variables, including Automation in Threat Detection ($r = 0.977$, $p < 0.01$), Data Processing Capacity (DPC) ($r = 0.982$, $p < 0.01$), and System Effectiveness (OSE) ($r = 0.980$, $p < 0.01$). These findings indicate that the more mature AI systems are, the more functional and responsive their capabilities as well as general performance related to health crisis management are.

Threat Detection Accuracy correlations with DPC ($r = 0.992$, $p < 0.01$) and ATD ($r = 0.987$, $p < 0.01$) turned out to be incredibly high, which confirms the idea that accurate and timely threat detection largely depends on the presence of good automation procedures and high data-processing capabilities. Inter-agency Collaboration Level (ICL) was statistically significant and positively correlated with all other portents, such as Incident Response Time ($r = 0.990$, $p < 0.01$). These results provide support for the significance of organizational coordination in improving the effectiveness of a system. A high validity was maintained between the Cybersecurity Resilience Index and TDA ($r = 0.991$, $p < 0.01$) and OSE ($r = 0.989$, $p < 0.01$); the greater the resilience of a system against cyber threats, the higher the effectiveness of its system and security on the health of the population. The correlation matrix shows that the structure is very coherent, where the advancements in one area (e.g., data capacity, automation, or collaboration) are closely linked to the ones in the rest. This congruence helps to demonstrate the construct validity of the model in question and substantiates the decision to have these components united in one comprehensive AI-driven health surveillance and response framework

Table 6. *Structural Model Results*

Hypotheses	SE	CR	P Value	Supported
ASM → TDA *(Positive correlation) (AI System Maturity → Threat Detection Accuracy)*	0.07949	*0.5469*	0.000	*Accepted*
ATD → IRT *(Negative correlation) (Automation in Threat Detection → Incident Response Time)*	0.7664	*0.2007*	0.000	*Rejected*
DPC → CRI *(Positive correlation) (Data Processing Capacity → Cybersecurity Resilience Index)*	0.8366	*0.2842*	0.000	*Accepted*
ICL → OSE *(Positive correlation) (Inter-agency Collaboration Level → Overall System Effectiveness)*	0.7930	*0.2842*	0.000	*Accepted*
TSD → OSE *(Positive correlation) (Training & Skill Development → Overall System Effectiveness)*	0.8367	*0.2542*	0.000	*Accepted*

Table 6. summarizes the results of a structural framework of testing the modeled relationships between the hypothetical constructs of the framework of AI-driven crisis management in health. Four of the five hypotheses show strong empirical support, as the latter has statistically significant paths ($p < .001$) and acceptable standard errors (SE). Hypothesis 1 of the analysis is confirmed, as there is a positive relationship where the AI System Maturity (ASM) and Threat Detection Accuracy are correlated, and the path coefficient ($CR = 0.5469$, $SE = 0.07949$, $p = 0.000$) is a positive value that shows that, as the systems using AI mature, there is a significant increase in the threat detection accuracy. This result highlights the role of developed AI infrastructures in identifying the possible health threats in an early and accurate manner. The second hypothesis, which implies a negative relationship between Automation in Threat Detection and Incident Response Time (IRT), is rejected, but it records a statistically significant p-value ($CR = 0.2007$, $SE = 0.7664$, $p = .000$). There is a low level of critical ratio and a high standard error, which indicates a lack of consistency in this relationship, and this could probably be due to a lack of consistency and efficiency in the automation process that may not equally reduce the number of response times. This relationship could be explained by the further refinement of the model or adding more mediating variables. The third hypothesis, which stated that there is a positive relationship between Data Processing Capacity (DPC) and Cybersecurity Resilience Index (CRI), was proved supported by an empirical value ($CR = 0.2842$, $SE = 0.8366$, $p = .000$). These findings indeed show that enhanced data processing, more so in real-time, would enhance the ability of a system to resist and respond to cyber and bio-surveillance threats.

The same way as in the case of Hypothesis 3, although at least as important, Hypothesis 4 was proven correct, indicating a positive correlation between the Inter-agency Collaboration Level (ICL) and System Effectiveness ($CR = 0.2842$, $SE =$

0.7930, p = .000). Such observation reinforces the value of institutional synergy and cross-sectoral collaboration in increasing the system-wide effects in a health crisis. Lastly, Hypothesis 5 was true wherein a substantial positive correlation between Training and Skill Development and System Effectiveness (OSE) was found out (CR = 0.2542, SE = 0.8367, p = .000). This emphasizes the vital importance of human capital and technical capacity building in maintaining the success of the deployment of AI and optimizing the results of its performance. Finally, this structural model confirms most of the theoretical assumptions, which the AI-based framework of public health is based on, which accompanies its feasibility with regards to a national level implementation and planning.

A. Interpretation of Results

These results obtained through the measurement, descriptive, correlational, and structural analysis (Table 22) offer strong evidence regarding the predictive power and the operating effects of AI-based elements within health crises management. In Table 2, AI System Maturity Level, Data Processing Capacity and System Effectiveness (OSE) constructs indicated high internal reliability (e.g., alpha = .922; alpha = .996) and acceptable loaded standardized (e.g., ASM Item 1 = .776), which confirms that these constructs are valid to use in modeling AI effectiveness. Nevertheless, only the relatively low AVE sizes (e.g., 0.4469 in the case of ASM and 0.4366 in the case of OSE) suggest the necessity of further enhancement of the convergent validity in the future, in terms of better indicators. Table 3 descriptive results indicate that the mean ratings of DPC (M = 3.01, SD = 1.35) and Incident Response Time (M = 2.99, SD = 1.23) are slightly higher in ranking as compared to other constructs, whereas OSE obtained the lowest ratings (M = 2.68), possibly implying a perceived performance gap concerning the system integration.

The values of the skewness and kurtosis of all the variables met the acceptable limits (e.g., skewness = 0.359; kurtosis = -1.292, ASM; DPC, respectively), which means that there is no severe aberration in terms of normality. Table 4 showed a significant and strong positive correlation between all the variables using correlation analysis ($p < .01$). As an example, the ASM had a strong correlation with the DPC (r = .982), TDA (r = .954), and OSE (r = .980), imply that AI maturity has a direct effect on various system outcomes. Remarkably, TDA too had a strong correlation with the DPC (r = .992), since computational infrastructure is an essential tool in determining predictive accuracy. Such strong dependencies denote the coherent framework, where the primary AI functions benefit each other in various operations. These relationships are further confirmed by means of structural model results in Table 5. The results supported the hypothesis via the test of hypotheses by showing that ASM was a significant predictor of TDA (CR = 0.5469, p = .000) and DPC was a significant enhancer of CRI (CR = 0.2842, p = .000).

ICL was identified to have positive impact on OSE (CR = 0.2842, p = .000), as well as TSD (CR = 0.2542, p = .000) proving the importance of inter-agency coordination and workforce development as associated with strategic issues. Nevertheless, the hypothesis concerning ATD and IRT was rejected, although it is considered to be statistically significant (CR = 0.2007, p = .000) probably because of the high variance and poor model fit (SE = 0.7664). Automation alone does not seem to have a positive effect on the number of incident response times unless there is better integration with the systems. Strategically, such outcomes imply that interventions ought to emphasize on AI system maturity, optimum data pipelines, inter-agency cooperation, and human capital formation. Meanwhile, care should be exercised against application of automation per se, which in complex, poorly integrated systems could have little to do with real-time responsiveness.

6. Discussion

In this study, empirical evidence is on the effectiveness of AI-based frameworks in national health crisis control. The structural model (Table 5) indicated that AI System Maturity and Data Processing Capacity became significant predictors of Threat Detection Accuracy and Cybersecurity Resilience Index. These findings reflect the importance of advanced AI systems and the resources of a solid data ecosystem in enhancing the ability to detect early and respond swiftly. The constructs Inter-agency Collaboration Level and Training & Skill Development proved to have a positive bearing on System Effectiveness (OSE), which means that cooperation among agencies and the competent employee base are the needed pillars of successful system implementation.

A large part of the findings is consistent with the prior literature. As an example, previous research by Topol (2019) and Rajkomar et al. (2019) pointed out the importance of AI to improve the accuracy of prediction and diagnosis in the sphere of public health. Equally, in the paper by Chen et al. (2021), researchers encountered the same idea that collaborative governance frameworks and multi-source data coordination elevate the resilience of the population in terms of health. Nevertheless, the

given study presents some new information, calculating such relationships with the help of structural modeling and transferring previous scholarly selection to empirical verification. One of the major differences is in the rejection of the hypothesis that a relationship exists between automation in threat detection and response time.

Findings of this research have immense ramifications for the field of public health policy and development of infrastructure. Policymakers are encouraged to focus on AI maturity that could be enhanced with powerful data pipelines and real-time analytics infrastructure. The key to achieving the potential of predictive systems will be investments in multi-agency coordination schemes and training programs for healthcare professionals. Technically, they should develop scalable and interoperable platforms that integrate with mobile health applications and emergency dashboards so that decision-makers take timely actions in times of outbreaks. Further on, data science teams should be strategically aligned with the authorities of public health to attend to their real-world implementation and policy proving.

AI tools do not have interoperability with current public health information systems, which disrupt or mangle the decision-making process. Second, there is a key issue of data governance, especially when systems lack data or are more decentralized, so that access becomes organized poorly or inconsistently. Third, a data gap between frontline health workers and policymakers narrows the number of advanced AI systems, but it needs a skill enhancement program. The efforts in this direction will be crucial in scaling the AI framework and its ethical, transparent, and efficient application in varying health systems.

7. Conclusion

The aim of this research was to propose and empirically justify a framework of AI-powered predictive analytics of nationwide health crisis management, with a view of highlighting real-time detection, cybersecurity resiliency, and inter-agency coordination. Measurement and structural model's analysis results (in Table 2 and 5), show that ASM, DPC, TSD, and ICL became significant predictors in determining system effectiveness. The conducted descriptive and correlational analyses (Tables 3 and 4) additionally revealed that these variables are highly interrelated and positively assessed by the respondents demonstrating that numerous people recognize the possibility of changing crisis management systems via AI implementation.

The study provides vital information to national policy by cybersecurity and public health that offers a data-based framework to incorporate AI into the monitoring of cyber-threats, epidemiological, and pandemic-response response activities. It shows that AI maturity and automation are a viable way to increase the threat detection accuracy and resilience which is a key to cyber-physical system integrity in the case of national crises. Using these insights as a start, AI-driven policy transformation could help governments go beyond reactively containing threats to attacking in a proactive, precision-based manner.

The results of this research, a number of strategic suggestions are promoted to improve the national health and cybersecurity crisis preparedness. There is an urgent requirement to design national AI cybersecurity standards, following ethical, privacy, and technical specifications. These norms will assist in controlling AI system implementation in crisis identification and reactions along with resourceful data management. The artificial intelligence-based threat intelligence centers must be formed that combine real-time information of the hospitals, social media sites, and the government.

These hubs will be used to coordinate a timely response as well as enhance a strengthened situational awareness between institutions. Third, upskilling and digital literacy initiatives are to be introduced, especially those of the cybersecurity and healthcare workforce. Closing the current skills gaps in the AI operation, data interpretation, and ethical governance, represented by the lower AVE scores in Table 2 and performance dependencies in Table 5, is necessary to optimize the system performance and informed decision-making in the real-world crisis circumstances.

The study has valuable contributions to AI-driven crisis management, such limitations have to be admitted. First of all, such an approach (use of self-reported data in the survey terms; see Table 3) presents a certain extent of bias in the responses, as the sample perceptions of participants might not always correspond to the real possibilities of systems and technical performance of such systems. The geographical concentration of the sample, in case it is confined to a certain country or region, encroaches on the validity of the results by compromising their similarity to any other setting or healthcare infrastructure country or nationally. Another weakness is associated with the measurement model itself since certain constructs demonstrated rather low Average Variance Extracted indicators (Table 2), which implies the necessity to improve the questions and criteria of measuring them in questionnaires in the future. Future studies will be important in overcoming these constraints in a bid to establish the applicability of the framework to a wider range of population and system contexts.

The future studies ought to concentrate on the coming age of technology and lasting effects on the system. An emerging perspective is the merging of quantum computing and blockchain security solutions into AI platforms to optimize the transparency of systems and their encryption and ability to ward off clever cyberattacks. The longitudinal research must be developed to determine the extent to which the AI-based crisis management policies need to be implemented and developed throughout the years to enable the researchers to analyze the scalability, efficacy, and sustainability of the policies in the real-life setting. The ethical governance structures specific to Crisis Technology and Information Systems have to be developed in extreme need. Such frameworks must devise strong policies regarding fairness, accountability, data privacy, and socially responsible use of AI so that technology advances in the fields of public health and cybersecurity become inclusive and socially responsible.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Goffer, M. A., et al. (2025). Cybersecurity and supply chain integrity: Evaluating the economic consequences of vulnerabilities in U.S. infrastructure. *Journal of Management World, 2025*(2), 233–243. https://doi.org/10.53935/jomw.v2024i4.907

[2] Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced cyber threats and cybersecurity innovation – Strategic approaches and emerging solutions. *Journal of Computer Science and Technology Studies, 5*(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9

[3] Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., … Hasan, R. (2025). AI-enhanced cyber threat detection and response advancing national security in critical infrastructure. *Journal of Posthumanism, 5*(3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965

[4] Hasan, S. N., Kaur, H., Mohonta, S. C., Siddiqa, K. B., Kaur, J., Haldar, U., … Manik, M. M. T. G. (2025). The influence of artificial intelligence on data system security. *International Journal of Computational and Experimental Science and Engineering, 11*(3). https://doi.org/10.22399/ijcesen.3476

[5] Barikdar, C. R., Siddiqa, K. B., Miah, M. A., Sultana, S., Haldar, U., Rahman, H., … Hassan, J. (2025). MIS frameworks for monitoring and enhancing U.S. energy infrastructure resilience. *Journal of Posthumanism, 5*(5), 4327–4342. https://doi.org/10.63332/joph.v5i5.1907

[6] Hassan, J., Rahman, H., Haldar, U., Sultana, S., Rahman, M. M., Chakraborty, P., … Barikdar, C. R. (2025). Implementing MIS solutions to support the national energy dominance strategy. *Journal of Posthumanism, 5*(5), 4343–4363. https://doi.org/10.63332/joph.v5i5.1908

[7] Moniruzzaman, M., Islam, M. S., Mohonta, S. C., Adnan, M., Chy, M. A. R., Saimon, A. S. M., … Manik, M. M. T. G. (2025). Big data strategies for enhancing transparency in U.S. healthcare pricing. *Journal of Posthumanism, 5*(5), 3744–3766. https://doi.org/10.63332/joph.v5i5.1813

[8] Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., … Hasan, R. (2025). AI-driven cybersecurity in IT project management: Enhancing threat detection and risk mitigation. *Journal of Posthumanism, 5*(4), 23–44. https://doi.org/10.63332/joph.v5i4.974

[9] Hasan, S. N., Hassan, J., Barikdar, C. R., Chakraborty, P., Haldar, U., Chy, M. A. R., … Kaur, J. (2023). Enhancing cybersecurity threat detection and response through big data analytics in management information systems. *Fuel Cells Bulletin, 2023*(12). https://doi.org/10.52710/fcb.137

[10] Hossin, M. E., Jahid, H., Chy, M. A. R., Hossain, S., Rozario, E., Khair, F. B., & Goffer, M. A. (2024). Harnessing business analytics in management information systems to foster sustainable economic growth through smart manufacturing and Industry 4.0. *Educational Administration: Theory and Practice, 30*(10), 730–739. https://doi.org/10.53555/kuey.v30i10.9643

[11] Goffer, M. A., Chakraborty, P., Rahman, H., Barikdar, C. R., Das, N., Hossain, S., & Hossin, M. E. (2024). Leveraging predictive analytics in management information systems to enhance supply chain resilience and mitigate economic disruptions. *Educational Administration: Theory and Practice, 30*(4), 11134–11144. https://doi.org/10.53555/kuey.v30i4.9641

[12] Sultana, S., Karim, F., Rahman, H., Chy, M. A. R., Uddin, M., Khan, M. N., Hossin, M. E., & Rozario,

E. (2025). AI-augmented big data analytics for real-time cyber attack detection and proactive threat mitigation. *International Journal of Computational and Experimental Science and Engineering*, *11*(3). https://doi.org/10.22399/ijcesen.3564

[13] Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowl Inf Syst 67, 6969–7055 (2025). https://doi.org/10.1007/s10115-025-02429-y

[14] Achuthan K, Ramanathan S, Srinivas S, Raman R., (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Front Big Data*. 7:1497535. doi: 10.3389/fdata.2024.1497535. PMID: 39703783; PMCID: PMC11656524.

[15] Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. *Frontiers in Big Data*, 7, 1497535. https://doi.org/10.3389/fdata.2024.1497535

[16] Alsmadi, I., & Zarour, M. (2020). Cybersecurity skills training and workforce development: A survey. *Computers & Security*, 97, 101970. https://doi.org/10.1016/j.cose.2020.101970

[17] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon) (371–390). *IEEE*. https://doi.org/10.23919/CYCON.2018.8405026

[18] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

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

[20] Cheung, S., Skopik, F., & Settanni, G. (2019). Collaboration in cyber threat intelligence sharing: Practices, challenges and research opportunities. *Computers & Security*, 87, 101589. https://doi.org/10.1016/j.cose.2019.101589

[21] European Union Agency for Cybersecurity (ENISA). (2021). Artificial intelligence and cybersecurity: Threat landscape. *ENISA*. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-threat-landscape

[22] Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011). Adversarial machine learning. In Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence (43–58). *ACM*. https://doi.org/10.1145/2046684.2046692

[23] Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

[24] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (305–316). *IEEE*. https://doi.org/10.1109/SP.2010.11

[25] Ujcich, B. E., Sanders, W. H., & Campbell, R. H. (2020). Toward resilient cyber infrastructures: Artificial intelligence, machine learning, and security. *ACM Computing Surveys*, 53(1), 1–36. https://doi.org/10.1145/3372023