World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Examining the Role of Artificial Intelligence in Strengthening Cyber Threat Intelligence Across U.S. Public Sector IT Infrastructure

Mariatu Mahmoud *, Barbara Aryeley Aryee and Kwadwo Adu Agyemang

Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA

World Journal of Advanced Research and Reviews, 2025, 28(03), 1476-1488

Publication history: Received on 03 November 2025; revised on 14 December 2025; accepted on 17 December 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4132

Abstract

Cyber threats targeting the U.S. public sector have escalated beyond the capacity of traditional security measures. Government agencies now face heightened vulnerability as they process vast amounts of sensitive data through increasingly complex technological infrastructures. This study investigates how artificial intelligence can enhance cyber threat intelligence throughout U.S. federal, state, and local government networks. A systematic literature review approach was employed, and peer-reviewed journal publications were searched across scientific databases, including IEEE Xplore, ScienceDirect, Scopus, and Web of Science, for government-enabled cybersecurity AI applications. The findings demonstrate that machine learning and deep learning capabilities dramatically increase the accuracy of threat detection, with organizations reporting a 75% reduction in the number of breaches because of implementing AI compared to those that do not rely on this technology. The quantitative metrics showed that AI-augmented models achieve detection rates with average accuracy scores of 1.000, successfully surpassing traditional signature-based techniques in uncovering advanced persistent threats and zero-day attacks. Notwithstanding, challenges such as budget considerations for 65.75% of institutions, IT workforce shortages for 55.25%, and the insecurities that come with integrating legacy systems into digital ones exist. This study establishes that the effective deployment of AI must be predicated on transparent training algorithms, greater inter-agency cooperation, adequate funding to modernize technical capabilities, train personnel, and compliance with regulatory frameworks, including FISMA, NIST standards, and adherence to the zero-trust architectural model, which are necessary prerequisites for robustly defending critical national infrastructure.

Keywords: Artificial Intelligence; Cyber Threat Intelligence; Public Sector Cybersecurity; Machine Learning; Threat Detection; Critical Infrastructure Protection

1. Introduction

The U.S. public sector is facing a surge of highly sophisticated cyber threats that have effectively outpaced and undermined traditional security countermeasures. The range of malicious cyberattacks is still dynamic and growing, which requires the premeditated design and execution of more sophisticated defensive frameworks. According to Godase (2025), the increasing complexity of modern cybercriminal activities calls for equally dynamic, intelligent, and proactive security systems. The amount of sensitive data, including citizen records, financial information, and national security intelligence, that public organizations keep and maintain is colossal, making cybersecurity in this space crucial for public safety and national security. With rapidly evolving cyber-attacks, new methods are required to reinforce security and privacy, as existing definitions of security are under constant testing (Kaur et al., 2024). The complexity and frequency of attacks have evolved beyond the capabilities of manual monitoring systems, which creates the need for advanced technological solutions.

* Corresponding author: Mariatu Mahmoud

Artificial intelligence offers an unprecedented chance to enhance the cyber defense of government operations. AI is an enabling technology for cybersecurity that enables automating repetitive jobs for the cybersecurity team, accelerating threat detection and response, as well as improving the accuracy of enhancing security posture (Jimmy, 2021; Adukpo & Bethel, 2025). Large amounts of data are processed using machine learning and deep-learning methods to identify patterns and outliers, which trigger a network alert on possible cyber-attacks in real-time (Jain & Mitra, 2025; Agboola & Alabi, 2025). The impact of deep learning on cybersecurity has been so enormous that defensive equipment that is deep learning-enabled continues to be leveraged to automatically detect cyber threats that improve and perform progressively and proficiently in no time (Salem et al., 2024). This new breed of AI technologies allows security teams to move from being reactive to being proactive, catching threats before they cause significant harm.

US public agencies have specific requirements that consist of advanced threat intelligence. Cyber-threats are changing, converging, and adapting in a manner that is becoming more difficult for traditional security methods to keep up with, especially as applied to critical infrastructure organizations (Rudner, 2013). In a broad sense, processing CTI is human-driven; it is analysts who wade through stacks of data to observe trends and evidence, but the amount of varied cyber threat intelligence (CTI) around the internet has exploded in volume, and they do not have time to process or react to CTI effectively (Alevizos & Dekker, 2024). The emerging mobile networks nowadays that serve as a foundation of modern life are now serving as central nervous systems to critical infrastructure and introducing new cybersecurity threats (Djenna et al., 2021). User behavior modeling, anomaly-based algorithms can detect malicious behaviors evidenced over a limited period, since threats from trusted agents are very hard to detect (Kim et al., 2019). The cases above illustrate what AI can offer the CTI operations for federal, state, and local government networks.

Notwithstanding, developing and deploying machine learning pipelines in cybersecurity has never been easy, as one needs to compose well-selected algorithms, find the right data containing the best features, besides continually enhance performance (Mohamed 2025). Although AI provides robust cybersecurity services, challenges are there, such as the computational resources needed, adversarial threat detection, and ethical issues that demand further exploration of trustworthiness and standardization of AI-based procedures (Shahana et al. 2024). There are major challenges for deep learning to be used in organoid analysis, including the need for a large amount of data to train, computational burden, and the probability of false positives or negatives (Najafabadi et al., 2015). In this article, we discuss how artificial intelligence (AI) in the form of machine learning, deep learning, and behavioral analysis can help enhance U.S. public sector IT systems with better cyber threat intelligence.

2. Methodology

This study adopts a systematic literature review process, which includes choosing main studies based on criteria and assessing the quality of the chosen publications. An exhaustive search of academic databases was undertaken using the PRISMA guidelines, including IEEE Xplore, ScienceDirect, Scopus, and Web of Science, to discover peer-reviewed literature directly relevant to artificial intelligence applications in cyber threat intelligence and cybersecurity in the United States. Primary studies were carefully picked by searching for reliable scientific sources using predetermined keywords such as artificial intelligence, machine learning, cyber threat intelligence, public sector cybersecurity, and government IT infrastructure.

3. Literature Review

The incorporation of artificial intelligence into cybersecurity operations signals a significant shift in how government agencies identify, prevent, and respond to cyber threats. This literature study investigates the present state of knowledge on AI technologies in cyber threat intelligence, as well as the unique challenges confronting the U.S. public sector IT infrastructure. The review is divided into four sections: artificial intelligence technologies in cyber threat detection and prevention, cybersecurity challenges and vulnerabilities in the U.S. public sector IT infrastructure, case studies of AI implementation in US federal and state government cybersecurity programs, and a quantitative analysis of the effectiveness of AI-enhanced threat detection on government networks. This review, which synthesizes existing research and practical findings, provides a solid basis for understanding how AI improves cyber threat intelligence capabilities while addressing the specific restrictions and requirements of public sector organizations.

3.1. Artificial Intelligence Technologies in Cyber Threat Detection and Prevention

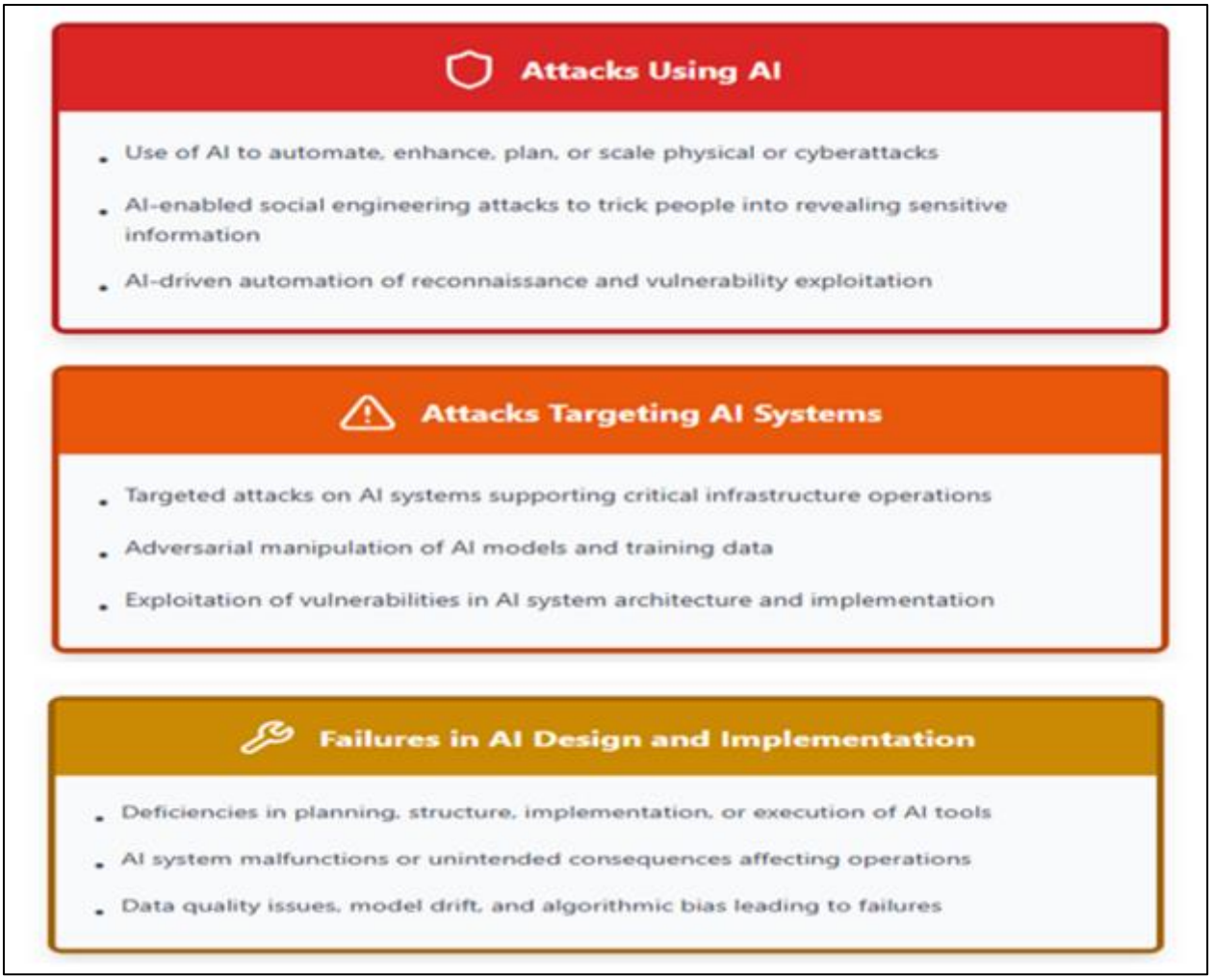
Traditional security methods are mostly based on permanent fixed security devices, such as firewalls and intrusion detection and prevention systems, and are proving inadequate to deal with the sophisticated reality of today's cyber-attacks (Mallick & Nath, 2024). The convergence of artificial intelligence and machine learning in cybersecurity marks a transformative stage, which enables advanced identification, response to, and mitigation of sophisticated cyber-

attacks (Jimmy, 2021). Machine learning and deep learning approaches in collaboration with heuristics of metaheuristic algorithms considerably advance the accuracy by which organizations can detect or respond to cyber threats (Diaba et al., 2023). Machine learning is also proving to be a powerful tool in the fight against data breaches and computer fraud, with the ability to analyze vast amounts of data, identify patterns, and bolster methods for detecting and defending against security threats (Okoli et al., 2024; Gokah et al., 2025). These AI-driven techniques have allowed cybersecurity to break away from just detecting known attack signatures but can now spot new types of attacks and zero-days that traditional systems could not uncover (Agboola, 2025).

Machine learning methods offer a range of solutions for cyber-attack detection and prevention using both supervised and unsupervised learning. Supervised methods like Random Forest and Gradient Boosting are used with high accuracy to detect attacks and classify between normal and malicious traffic (Bagadi & Adimulam, 2025). Unsupervised algorithms, such as clustering, have been successful in detecting network traffic anomalies using unlabeled data, and making it favorable for environments where threat information is scarce (Vikram, 2020). Furthermore, unsupervised techniques are attractive as they might be able to identify new attacks without being constrained by labelled datasets, which are known to be difficult to obtain in cybersecurity due to the dynamism of threats and the high cost of manual labelling (Usama et al., 2019). Some recent approaches with unsupervised anomaly detection models exclusively based on normal data have shown good results for enhancing zero-day attack identification targeting critical infrastructures (Pinto et al., 2024). These methods permit security systems to adjust to new threats without undue human intervention.

Deep learning technologies have transformed the traditional intrusion detection and malware detection capabilities in today's cybersecurity systems. Deep neural networks can enable accessibility to sensor data at all levels of the network stack and define a flexible intrusion detection system with resilience learning ability and be able to detect new or zero-day features in network behavior, thus ejection intruders into the system and minimizing the chance of compromise (Reddy et al., 2024). Convolutional neural networks are commonly employed in network traffic for feature extraction, especially spatial ones, while recurrent neural networks and long short-term memory models are successful only on the sequential data and capture spatial-temporal dependences, especially complex patterns of attack detection (Sharma et al., 2025). Deep learning includes a family of machine learning algorithms that employ the use of artificial neural networks to learn hierarchical representations of data in multiple levels corresponding to different levels of abstraction and involving deep structures with many hidden layers (Taye, 2023). Artificial neural networks also outperform traditional machine learning classifiers in intrusion detection systems, giving good accuracy, recall for binary as well as multiclass estimation of network attacks (Alharthi et al., 2025).

Conceptually, natural language processing has been shown to provide effective technology to improve cyber threat intelligence analysis and tune automatic response capabilities. Through applications of natural language processing, including named entity recognition, sentiment analysis, topic modeling, and machine learning-based threat detection, organizations can better detect, respond to, and mitigate cybersecurity risks (Kundiya & Haribhakta, 2025). Natural language processing provides powerful methods and techniques for improving analysis, detection, and response to cybersecurity incidents by deriving useful information from unstructured sources like security logs, threat reports, and online forums (Sharma & Arjunan, 2023). Modern natural language processing methods leverage pre-trained transformer models, such as fine-tuned versions of BERT architectures and syntactic dependency parsing used for automatic threat intelligence extraction from threat reports, blogs, and advisories (Jumaniet al., 2025). Large language models are becoming technology that enhances cyber threat intelligence by automating threat discovery and analyzing data, as well as alerting insights in real-time with much higher accuracy, response time, and level of contextual understanding than traditional methods (Kovalchuck et al., 2025). These natural language processing functions enable security teams to ingest a large volume of text-based threat intel data at a rate that would be impossible for human analysts.



Source: U.S. Department of Homeland Security. (2024).

Figure 1 CISA's Three Categories of Cross-Sector AI Risks to Critical Infrastructure

Figure 1 illustrates the three primary categories of cross-sector artificial intelligence risks to U.S. critical infrastructure as identified by the Cybersecurity and Infrastructure Security Agency in 2024. The first category encompasses attacks using AI, where adversaries leverage artificial intelligence to automate, enhance, and scale cyberattacks, including social engineering and vulnerability exploitation. The second category addresses attacks targeting AI systems themselves, involving adversarial manipulation of AI models, training data poisoning, and exploitation of vulnerabilities in AI system architectures. The third category focuses on failures in AI design and implementation, including deficiencies in planning and execution, system malfunctions, and data quality issues that lead to operational failures in critical infrastructure operations.

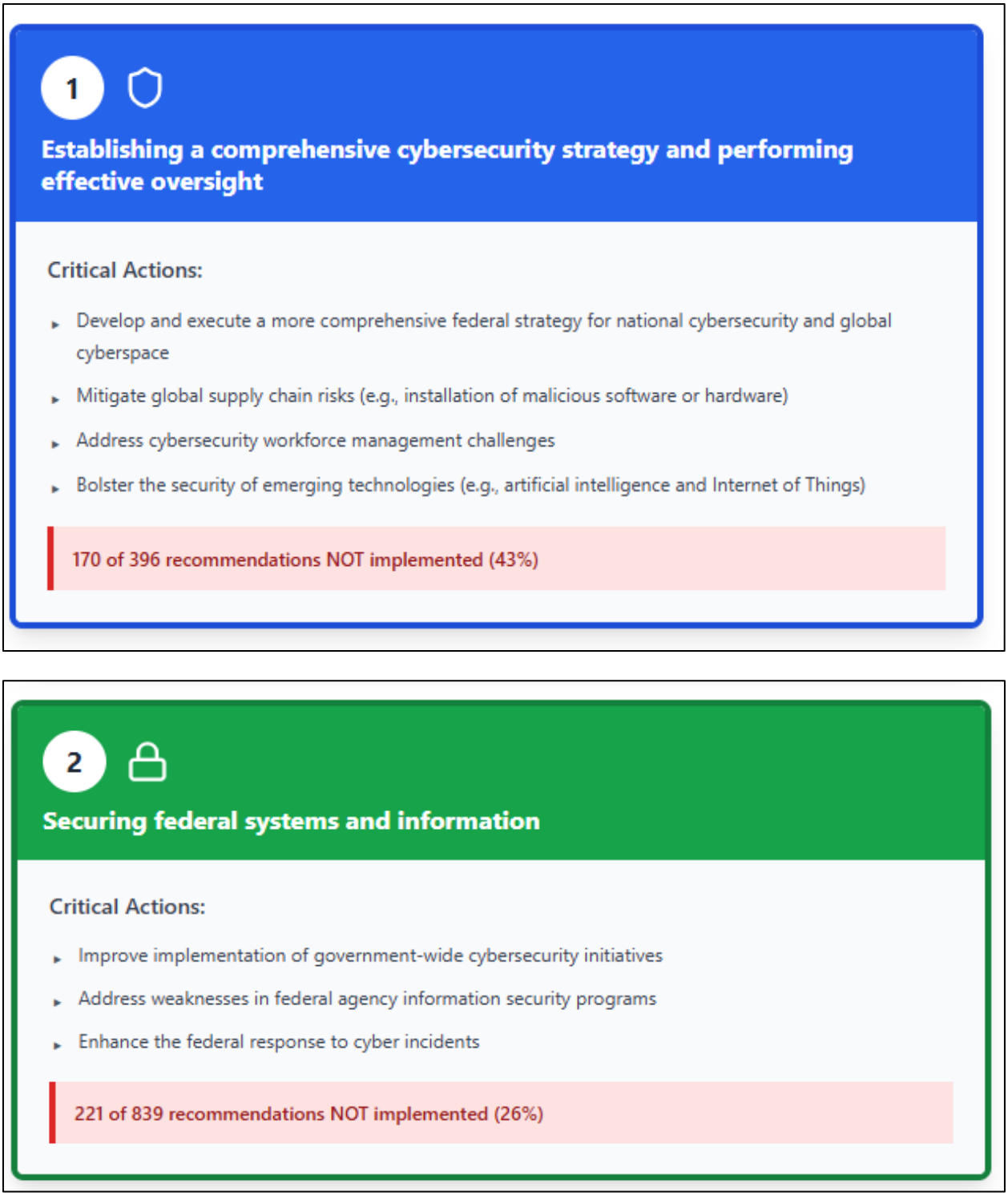
3.2. Cybersecurity Challenges and Vulnerabilities in U.S. Public Sector IT Infrastructure

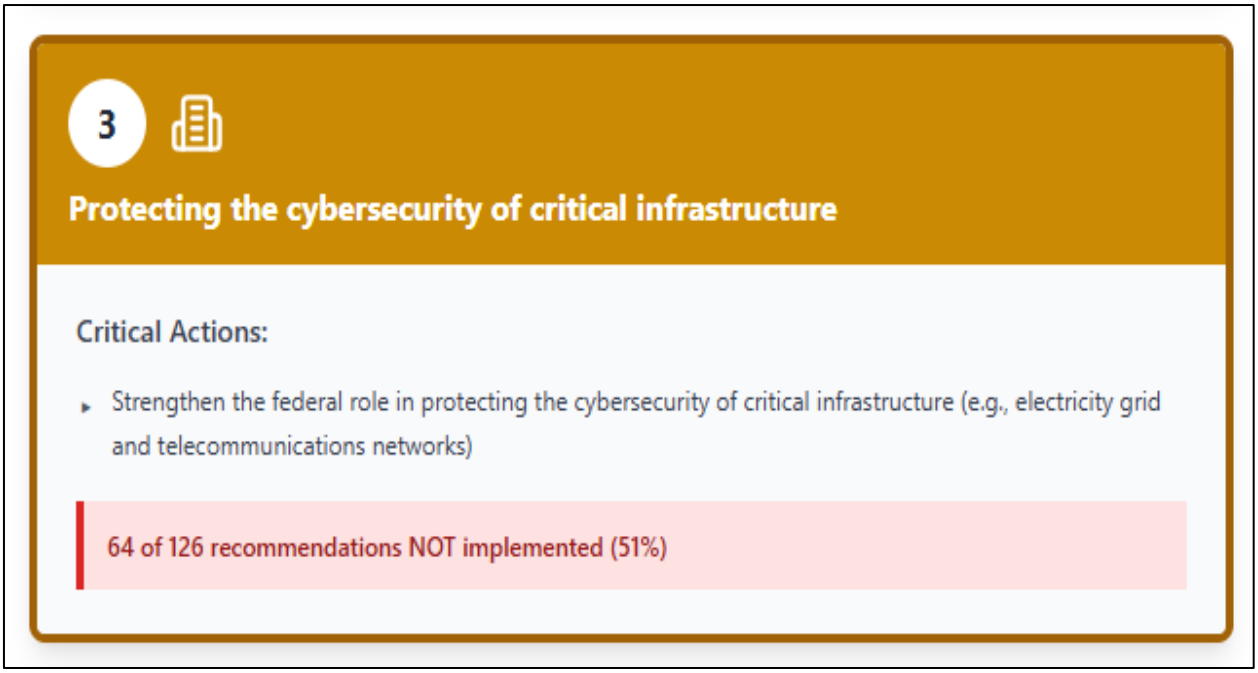
The development of cyber threats against public institutions has grown rapidly over the past twenty years, ranging from basic malware attacks to highly advanced operations. In the 1980s, the first major malicious software threat emerged, with the Morris worm gaining widespread media attention; it infected over 6,000 computers and caused damages estimated between $100,000 and millions of dollars (Parikh, 2019; Ajayi-Kaffi et al, 2025). By the mid-2000s, a series of cyberattacks known as Titan Rain targeted various U.S. government and military agencies, as well as businesses in other countries, and was believed to be linked to hackers in China (Iftikhar, 2014). Advanced persistent threats mark a major evolution in cybercrime, involving highly sophisticated operations designed to implant or extract sensitive data or disrupt complex networks (Abdullah et al., 2025). The 2020 SolarWinds attack revealed the considerable power of state-sponsored actors to exploit supply chain vulnerabilities on a global scale, which affected thousands of organizations worldwide. It underscored how governments increasingly use cyber-attacks as tools for espionage and influence (Butler et al., 2024; Sani & Aryee, 2025; Akande & Enyejo, 2023).

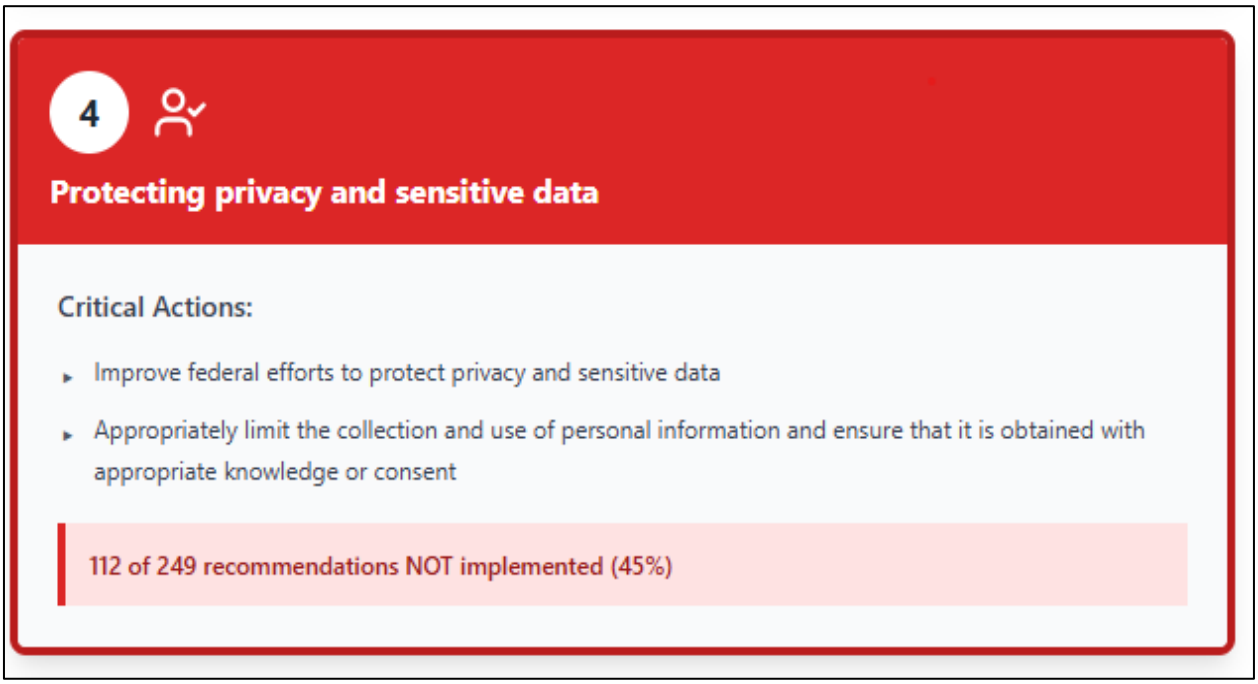
Rigid legacy infrastructure offers vulnerabilities across all aspects of federal, state, and local government IT environments. Rare is a critical infrastructure ecosystem that does not contain legacy systems declared at end-of-life or unsupported and outdated software or operating systems for which the security officers are held responsible and accountable, but is a risky blind spot (Dryland, 2022). The federal government spends over $100 billion on IT each year, the majority of which is spent to operate and maintain current systems, and agencies have historically reported spending around 80% on maintenance and portfolio operations, including maintenance for legacy systems that are difficult to address, like rising costs and cybersecurity risks (Zhao et al., 2019). Outdated software that is built without adequate processing power, logging capabilities, and real-time data-sharing to underpin the sophisticated security measures required to protect local governments from even more advanced malware, ransomware, and cyberattacks (Pemmasani & Rock, 2023). Studies showed that the legacy systems being used, as well as the decreasing amount of segmentation, still determine weaknesses for integrated AI-based security solutions in cyber threat infrastructures (Hurst & Shone, 2024).

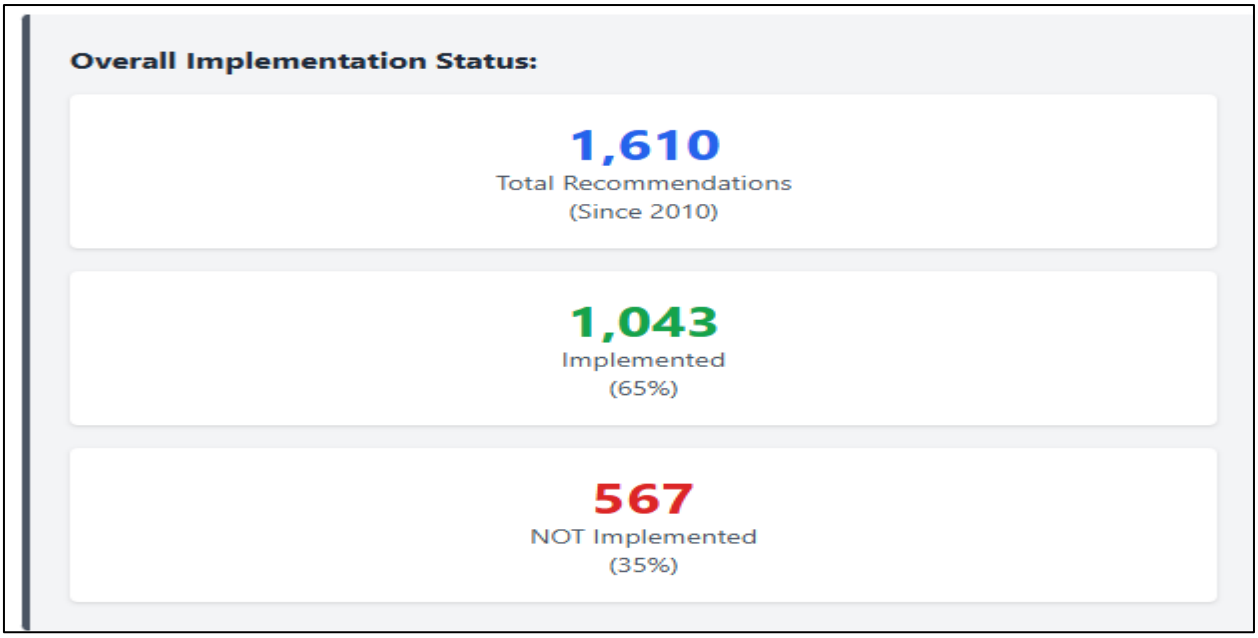
Regulatory frameworks and compliance regulations have adapted to the emerging cybersecurity threats with extensive standards and architectures. The Federal Information Security Modernization Act of 2014 (FISMA) charges NIST with the responsibility for developing information security standards and guidelines, including minimum requirements for federal systems (Maclean, 2017). Zero trust refers to a collection of cybersecurity paradigms that cut down the migrated detection-based perimeter protection approach, which considers users, assets, and resources without necessarily trusting any, if not explicitly granted based on certain conditions invoking their physical or network placement (Kim et al., 2024). By enhancing FISMA with the NIST SP 800-53v5 and FedRAMP, the U.S. government can develop a consistent, unified approach to federal cybersecurity efforts that are truly whole-of-government. Key highlights include clarifying federal cybersecurity roles for improved cooperation for intra-and inter-agency relationships and advancing risk-based cybersecurity posture. The federal zero trust architecture strategy demands agencies to meet certain real-time cybersecurity standards and objectives, which places significant emphasis on strong enterprise identity and access controls, including multi-factor authentication, encrypting all network traffic, and establishing rules allowing messages between components only if specific conditions are met (Mensah, 2024). The Pentagon's requirement for NIST zero trust architecture complements its standing with Cybersecurity Maturity Model Certification (CMMC) mandate, which requires federal agencies to implement these principles by the end of the 2027 fiscal year (Grad, 2024).

Sharing information and the workforce challenges impact government cybersecurity resiliency at all levels. The exchange of information is central to advancing the nation's cybersecurity because it requires collaboration between cooperation among numerous entities and organizations, including programs that facilitate near real-time distribution of machine-readable cyber threat indicators and defensive measures (Asiri et al., 2023; Aryee et al, 2025). Persistent challenges like security and timeliness complicate information sharing with nonfederal partners, who noted that the FBI had briefed them on a cyber threat five months after it was discovered (Bakis & Wang, 2017). Evidence from the literature indicates that much of the information distributed by federal government agencies and departments is either not being used or used inefficiently, despite government agencies having a unique opportunity to share significant amounts of cybersecurity data at little cost (Rodin, 2015; Akande & Enyejo, 2024). The skills gap in the worldwide cyber arena has become a big problem. (Spates, 2024). The United States was projected to have a deficit of approximately 314,000 cybersecurity professionals, given that the total employed cybersecurity workforce in the United States is only 716,000, and employers had found that most graduates from multiple programs were often deficient in basic knowledge, field experience, and essential interpersonal skills (Crumpler & Lewis, 2022).


1
Establishing a comprehensive cybersecurity strategy and performing effective oversight
Critical Actions:
Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace
Mitigate global supply chain risks (e.g., installation of malicious software or hardware)
Address cybersecurity workforce management challenges
Bolster the security of emerging technologies (e.g., artificial intelligence and Internet of Things)
170 of 396 recommendations NOT implemented (43%)
2
Securing federal systems and information
Critical Actions:
Improve implementation of government-wide cybersecurity initiatives
Address weaknesses in federal agency information security programs
Enhance the federal response to cyber incidents
221 of 839 recommendations NOT implemented (26%)


3
Protecting the cybersecurity of critical infrastructure
Critical Actions:
Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks)
64 of 126 recommendations NOT implemented (51%)


4
Protecting privacy and sensitive data
Critical Actions:
Improve federal efforts to protect privacy and sensitive data
Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent
112 of 249 recommendations NOT implemented (45%)



U.S. Government Accountability Office. (2024).

Figure 2 Four Major Cybersecurity Challenges and 10 Associated Critical Actions

Figure 2 depicts four main cybersecurity threats facing the United States federal government, as well as 10 critical actions outlined in the Government Accountability Office's 2024 High-Risk Series study. The first challenge is developing a comprehensive cybersecurity plan, with 43% of advice not implemented. The second problem is to secure government systems and improve incident response, with 26% of recommendations still unfinished. The third and fourth problems are focused on critical infrastructure cybersecurity and preserving privacy and sensitive data, with implementation gaps of 51% and 45%, respectively. Despite these shortcomings, federal agencies have responded to 1,043 of 1,610 recommendations since 2010, which indicates that there is still more work to be done.

3.3. Case Studies of AI Implementation in U.S. Federal and State Government Cybersecurity Programs

A study by Adewusi et al. (2024) explored the use of artificial intelligence in the U.S. federal cybersecurity infrastructure and the effectiveness of machine learning, natural language processing, and neural networks in strengthening vital systems against new cyber threats. Their study showed that the applications of AI in defense and national cybersecurity contribute to increasing the speed and accuracy of detection, preventing threats from evolving by providing an automated response. Their research highlighted that AI-based cybersecurity applications, such as anomaly detection, predictive analytics, and threat intelligence, have been in use across the federal government to protect critical national infrastructure. Their results indicated that AI technologies used in the United States play a key role in strengthening national infrastructure by providing faster threat detection and response than traditional security systems can offer.

Research by Eze et al. (2025) analyzed the impact of artificial intelligence on policy outcomes within the United States' cybersecurity policy from a review of policy plans, threat assessments, and technological capabilities at agencies across the federal government. Their research demonstrated that AI is a fundamental component in the cybersecurity readiness plan, as well as providing unmatched technology for threat identification, response automation, and predictive analysis in the federal government. By analyzing existing practices and policy blueprints, their study illustrated that an effective AI adoption in national cybersecurity should be measured by addressing both innovative technology solutions, policies, public-private partnership (PPP) frameworks, and international collaboration.

Another study by Obioha (2024) looked at the state-level implementation of AI in private sector organizations and public institutions, particularly educational technology systems and cybersecurity programs for U.S. public schools. Their Logistic regression analysis from K-12 Cybersecurity Resource Center data indicated that AI systems make schools 75% less likely to suffer from breaches, which indicates a substantial protective role of AI-based security mechanisms. Their study found that AI-enabled security tools, including threat detection algorithms and anomaly-detection features, contribute to schools' ability to monitor network traffic and recognize potential breaches in real time, with a comparative analysis of FERPA- and COPPA-compliance reports showing that the rate of privacy violations

was significantly lower among schools using AI, with 0.57 average violations per school compared 1.50 in schools without AI.

Furthermore, research by Virk et al. (2024) investigated the adoption of AI in the healthcare cybersecurity ecosystem, including performance metrics and lessons learned from implementations across public healthcare organizations in the U.S. The authors highlighted that AI penetration in healthcare provides support with big data sets of patients, transition to big data on cases, access to information for patient history and surgeries, data on and simulation for surgery, and the ability of clinical decision support while still addressing security trends. The results of their study also highlighted that transparency on AI algorithms' training and their analytical approach is essential in allowing professionals to place trust in any kind and make informed decisions about applying AI results with more robust digital policy and data protection guidelines. This provides another layer or shield for sensitive data. Their study concluded that with the growing digitization of public sector services, advancing cybersecurity through system monitoring, cybersecurity training, and enhanced collaboration among different regions and systems will allow effective and safe implementation of AI while improving security outcomes.

3.4. Quantitative Analysis of AI-Enhanced Threat Detection Effectiveness in Government Networks

A study conducted by Eleweke et al. (2024) demonstrated the efficiency of machine learning models in making AI software embedded in critical infrastructure, such as energy, transportation, and healthcare systems. Their study used two ensemble machine learning models, Random Forest and Gradient Boosting, to discriminate malicious PortScan traffic from Friday Afternoon Port Scan (FRAP) in the NSL-KDD dataset. Their findings indicated that both models attained the perfect classification performance, as all performance evaluation measures (including accuracy, precision, recall, F1, and ROC-AUC values scored 1.000) have shown a non-discriminatory low detection of threats. The misclassification rates were very low according to the confusion matrix analysis, in which acquiring the technology of Random Forest was slightly better than that of Gradient Boosting. A forward packet characteristic was revealed as more significant in the decision process through feature importance plots, which indicated that the model pinpointed several key network anomalies. This discovery adds measurable proof to the fact that AI-enriched deployments can outperform traditional signature-based detection measures used to detect malicious activities on government networks.

Similarly, research by Nakayenga et al. (2024) analyzed the disruptive potential of AI to improve public safety and emergency management, including U.S. government infrastructures and systems through various AI-based predictive analytics, machine learning models, and sophisticated threat detection algorithms. Their results revealed that AI systems can use IoT sensors, social media, environmental data, and crime statistics in real-time, thereby lowering response time, predicting public safety threats and optimizing resource allocations. Their study provided quantitative evidence that from 1980 to 2024, the U.S. has had at least 387 weather and climate disasters with damages exceeding $1 billion, totaling more than $2.74 trillion in damages, which demonstrates a dire demand for AI-enhanced disaster response systems. Their research also shows that AI solutions allow law enforcement, emergency management, and cybersecurity organizations to move from a reactive posture to a proactive stance with intelligence-driven operations to dramatically improve threat mitigation success rates throughout federal, state, and local government departments.

Additionally, Kezron (2024) proposed a Trust-by-Design cybersecurity framework for AI-driven systems in critical infrastructures, based on NIST Cybersecurity Framework domains of Identify, Protect, Detect, Respond, and Recover. After performing a systematic literature review on 2,395 publications after filtering 236 peer-reviewed sources, their work identified AI cybersecurity use cases for intrusion detection, behavior analysis systems, access control systems, and blockchain-based audit, along with automated recovery systems. Their research provided empirical proof that AI-enabled integration, along with each of the NIST framework domains, significantly accelerates response time and enhances thoroughness in threat detection for high-risk sectors such as smart manufacturing and healthcare systems. Their study also found fundamental empirical validation gaps and called for pilot testing in government settings to quantify specific improvements of false positive rate, false negative rate, and cost-benefit analysis regarding AI operationalization across different public sector bodies (Ajayi-Kaffi, 2024).

Another study conducted by Haque (2024) explored the use of AI systems in urban mobility infrastructure networks and their impact on transport safety based on U.S. cities. The researcher used a systematic review method and reviewed peer-reviewed articles, government documents, and transportation reports for the past 20 years. Their results showed that machine-learning-based reinforcement-learning methods and deep learning frameworks were able to yield significant gains in the individual performance metrics. These AI-augmented systems, including congestion minimization, fuel optimization, emissions reduction, proactive risk-sensing safety solutions, and adaptive control, ensured reduced travel delay and traffic disruption. INTERflex decreased energy consumption and enhanced security as well. US city use cases also showed that when AI applications were integrated with smart infrastructure and

connected vehicle tech, they facilitate dynamic route optimisation and congestion management. They delivered faster response times to incidents and improved the speed with which they were able to mitigate threats. Their study demonstrated with quantifiable evidence that AI-augmented simulation-based systems surpassed conventional methods for detection accuracy, operation efficiency, and cost in traffic management.

4. Conclusion

This study demonstrates that artificial intelligence and machine learning technologies hold transformative potential for cybersecurity intelligence generation within U.S. public sector information technology systems. These technologies enhance detection accuracy, accelerate response times, and strengthen predictive analysis capabilities. The research findings indicate that AI has evolved from an optional enhancement to an essential requirement for contemporary cybersecurity operations. AI-supported detection capabilities, when combined with skilled professional expertise, identify threats that traditional methods and technologies struggle to detect accurately and efficiently. AI-powered solutions deliver improved threat detection rates alongside significant reductions in overall cybersecurity risk exposure. Evidence from federal, state, and local government implementations reveals several critical requirements for successful AI integration. These include transparent algorithm training processes, enhanced inter-agency data sharing mechanisms, sustained investment in technology infrastructure upgrades, comprehensive personnel training programs, and strict adherence to established regulatory standards such as FISMA, NIST frameworks, and Zero Trust Architecture principles. Future research should address several important areas. These include the development of standardized performance metrics for AI-driven cybersecurity systems, longitudinal studies examining AI effectiveness across different governmental organizational levels, and comprehensive frameworks that balance technological innovation with ethical considerations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., binte Ashfaq, E., & Muhammad, Z. (2025). Analytics-Driven Insights into Cybercrime Evolution, Trends, and Defense Strategies: A Comprehensive Survey.

[2] Adukpo, T. K., & Bethel, J. O. (2025). Impact of macroeconomic factors on government spending in Ghana. American Journal of Applied Statistics and Economics, 4(1). https://doi.org/10.54536/ajase.v4i1.5833

[3] Agboola, O. K. (2025). AI-driven fraud detection and biometric KYC: Enhancing ethical compliance in U.S. digital banking. International Journal of Computer Applications Technology and Research, 14(8), 112–121. https://doi.org/10.7753/IJCATR1408.1010

[4] Agboola, O. K. (2025). Auditing bias in AI and machine learning-based credit algorithms: A data science perspective on fairness and ethics in FinTech. International Journal of Technology Management, 11(2), Article 10. https://doi.org/10.21590/ijtmh.11.02.10

[5] Agboola, O. K. (2025). The role of behavioural economics in understanding and countering fraudulent tactics. IOSR Journal of Economics and Finance, 16(4, Series 1), 8–12. https://doi.org/10.9790/5933-1604010812

[6] Agboola, O. K., & Alabi, K. O. (2025). Predicting systemic financial crises with AI and machine learning: A macroprudential data science approach in the US context. International Journal of Research Publication and Reviews, 6(8), 5121–5136.

[7] Ajayi-Kaffi, O. V. (2024). Is Agile methodology better than waterfall approach in enhancing effective communication in healthcare process improvement projects? International Journal of Research Publication and Reviews, 5(11), 3648–3651.

[8] Ajayi-Kaffi, O., Emmanuel, I., Azonuche, T. I., & Ijiga, O. M. (2025). Agile-Driven Digital Transformation Frameworks for Optimizing Cloud-Based Healthcare Supply Chain Management Systems. International Journal of Scientific Research and Modern Technology, 4(5), 138–156. https://doi.org/10.38124/ijsrmt.v4i5.1002

[9] Alharthi, A., Alaryani, M., & Kaddoura, S. (2025). A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. Array, 100406.

[10] Aryee, B. A., Agyemang, K. A., & Mahmoud, M. (2025). Enhancing operational efficiency of U.S. healthcare data centers through advanced analytics and automation. Finance & Accounting Research Journal, 7(10), 524–539. https://doi.org/10.51594/farj.v7i10.2102

[11] Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. ACM transactions on cyber-physical systems, 7(2), 1-33.

[12] Bagadi, G. R., & Adimulam, Y. B. (2025, March). Random Forest and Gradient Boosting for Superior Intrusion Detection and Anomaly Classification. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1618-1625). IEEE.

[13] Bakis, B. J., & Wang, E. D. (2017). Building a national cyber information-sharing ecosystem.

[14] Buckley, R. (2025). A cyber situation awareness framework for sectoral ISACs: enhancing cyber information sharing at strategic and policy levels (Doctoral dissertation, University of Limerick).

[15] Butler, P., Kelley, J., Ellis, J., & Olatunbosun, S. (2024, July). Cybersecurity Threats: An Analysis of the Rise and Impacts of State Sponsored Cyber Attacks. In World Congress in Computer Science, Computer Engineering & Applied Computing (pp. 187-194). Cham: Springer Nature Switzerland.

[16] Crumpler, W., & Lewis, J. A. (2022). Cybersecurity workforce gap (p. 10). Center for Strategic and International Studies (CSIS).

[17] Diaba, S. Y., Shafie-Khah, M., & Elmusrati, M. (2023). Cybersecurity in power systems using meta-heuristic and deep learning algorithms. IEEe Access, 11, 18660-18672.

[18] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cybersecurity issues of critical cyber infrastructure. Applied sciences, 11(10), 4580.

[19] Dryland, L. (2022). Eliminating the blind spots: How to be accountable for an organisation's overall security. Cybersecurity: A Peer-Reviewed Journal, 5(4), 350-360.

[20] Eleweke, I., Ugboko, R., Omotosho, O., Abbas, R., Adesokan, A., & Isibor, I. P. (2025) Strengthening security, privacy, and trust in artificial intelligence software for critical infrastructure in the United States.

[21] Godase, V. (2025). Navigating the digital battlefield: An in-depth analysis of cyber-attacks and cybercrime. International Journal of Data Science, Bioinformatics and Cybersecurity, 1(1), 16-27.

[22] Gokah, B. E., Amoako, E. K., Adom, S. G., Abakah, L. K., & Sampson, E. (2025). AI-driven user experience (UX) frameworks to enhance trust and security in U.S. online banking. Finance & Accounting Research Journal, 7(9), 465–478. https://doi.org/10.51594/farj.v7i9.2069

[23] Grad, A. (2024). Nonprofit Cybersecurity: NIST CSF 2.0 as Exemplar of Zero-Trust Architecture. University of New Hampshire.

[24] Haque, M. M. (2025). Systematic Review on The Impact Of AI-Enhanced Traffic Simulation On US Urban Mobility And Safety. ASRC Procedia: Global Perspectives in Science and Scholarship, 1(01), 833-861.

[25] Hurst, W., & Shone, N. (2024). Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation. In Management and Engineering of Critical Infrastructures (pp. 265-286). Academic Press.

[26] Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772.

[27] Jain, V., & Mitra, A. (2025). Real-time threat detection in cybersecurity: leveraging machine learning algorithms for enhanced anomaly detection. In Machine Intelligence Applications in Cyber-Risk Management (pp. 315-344). IGI Global Scientific Publishing.

[28] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 1, 564-74.

[29] JOSHUA, E. (2022). CYBER THREATS IN THE MODERN ERA: AN IN-DEPTH ANALYSIS.

[30] Jumani, A., Baig, A., Akhtar, E. D. S., Shamim, M. S., Zaheer, H., & Changaiz, A. (2025). AUTOMATING CYBER THREAT INTELLIGENCE EXTRACTION USING NATURAL LANGUAGE PROCESSING TECHNIQUES. Kashf Journal of Multidisciplinary Research, 2(06), 184-201.

[31] 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.

[32] Kazeem, T., Agboola, O. K., Okika, N., Owoola-Adebayo, S. F., Opeola, F., Akunna, N. L., & Abimbola, O. S. (2025). Risk management and governance in blockchain-based digital identity projects: A business analysis and project management framework. ITEGAM–Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA), 11(54). https://doi.org/10.5935/jetia.v11i54.1710

[33] Kezron, I. E. (2025). Novel cybersecurity framework for AI-driven drone integration by critical SMEs in economically distressed US rural communities: Advancing secure precision operations in high-risk environments. Well Testing Journal, 34(S3), 1-44.

[34] Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. Applied Sciences, 9(19), 4018.

[35] Kolluri, V. (2024). Revolutionary research on the ai sentry: an approach to overcome social engineering attacks using machine intelligence. International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, 1(1), 53-60.

[36] Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis. Вісник Черкаського державного технологічного університету, 30(1), 48-58.

[37] Kundiya, K., & Haribhakta, Y. (2025). A systematic review on insider threat detection using natural language processing. International Journal of Information Security, 24(6), 227.

[38] Lee, T. (2024). A Comprehensive Analysis of Challenges and Strategies in Enhancing Cybersecurity for the Defense Industry.

[39] Maclean, D. (2017). The NIST risk management framework: Problems and recommendations. Cybersecurity: A Peer-Reviewed Journal, 1(3), 207-217.

[40] Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1-69.

[41] Mensah, F. (2024). Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity. International Journal of Academic and Industrial Research Innovations (IJAIRI), 10, 339-346.

[42] 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, 1-87.

[43] Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. Journal of big data, 2(1), 1.

[44] Nakayenga, H. N., Akashaba, B., Twineamatsiko, E., Zimbe, I., Ssetimba, I. D., Bagonza, J. K., & Pinyi, E. O. (2024). Leveraging AI for real time crime prediction, disaster response optimization and threat detection to improve public safety and emergency management in the US. World journal of advanced research and reviews, 23(3).

[45] Obioha Val, O. (2024). The Role of Artificial Intelligence (AI) in Enhancing Cybersecurity for Educational Technologies in US Public Schools. Asian Journal of Research in Computer Science, 17(11), 10-9734.

[46] Ogunjide, J., Oluwatobi, Awowole, A. O., Adamaagashi, I., Prince, & Agboola, O. K. (2025). Relationship between biometric technology and customer satisfaction in the fintech sector. IIARD International Journal of Economics and Business Management, 11(4), 190–204. https://doi.org/10.56201/ijebm.vol.11.no4.2025.pg190.204

[47] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295.

[48] Oluomachi, E., Ahmed, A., Ahmed, W., & Samson, E. (2024). Assessing the effectiveness of current cybersecurity regulations and policies in the US. arXiv preprint arXiv:2404.11473.

[49] Parikh, A. (2019). Cloud security and platform thinking: an analysis of Cisco Umbrella, a cloud-delivered enterprise security (Doctoral dissertation, Massachusetts Institute of Technology).

[50] Pemmasani, P. K., & Rock, D. (2023). The Impact of Ransomware on Government Agencies: Lessons Learned and Future Strategies. International Journal of Modern Computing, 6(1), 64-74.

[51] Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2024). Enhancing Critical Infrastructure Security: Unsupervised Learning Approaches for Anomaly Detection. International Journal of Computational Intelligence Systems, 17(1), 236.

[52] Rains, T. (2023). Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization. Packt Publishing Ltd.

[53] Reddy, S. P. K., Nagavelli, U., Kiran, Y. S., Kondoju, C. S., Bushmoni, S., & Yashaswi, A. (2024, December). Deep Learning for Zero-Day Threat Detection and Mitigation. In 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS) (pp. 1362-1368). IEEE.

[54] Rodin, D. N. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. Public Contract Law Journal, 44(3), 505-528.

[55] Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453-481.

[56] 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(1), 105.

[57] Sani, Z. N., & Aryee, B. A. (2025). Optimizing drug supply chains to prevent shortages in rural U.S. hospitals. EPRA International Journal of Economics, Business and Management Studies. https://doi.org/10.36713/epra24022

[58] Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Mahmud, M. A. A., Johora, F. T., & Suzer, G. (2024). AI-driven cybersecurity: Balancing advancements and safeguards. Journal of Computer Science and Technology Studies, 6(2), 76-85.

[59] Sharma, H., Kumar, P., & Sharma, K. (2025). Intelligent Time Series Analysis for Intrusion Detection in the Internet of Things: A Generative-Adversarial-Network-Enhanced Convolutional-Neural-Network–Long-Short-Term-Memory Framework Using Signal Features. Intelligent Computing, 4, 0127.

[60] Sharma, S., & Arjunan, T. (2023). Natural language processing for detecting anomalies and intrusions in unstructured cybersecurity data. International Journal of Information and Cybersecurity, 7(12), 1-24.

[61] Spates, M. (2024). *Remedying the Cybersecurity Employment Gap-The Job Seekers' Perspective: A Qualitative Study* (Doctoral dissertation, Capitol Technology University).

[62] Taye, M. M. (2023). Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. *Computers*, *12*(5), 91.

[63] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access*, *7*, 65579-65615.

[64] Vikram, A. (2020, June). Anomaly detection in network traffic using unsupervised machine learning approach. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)* (pp. 476-479). IEEE.

[65] Virk, A., Alasmari, S., Patel, D., & Allison, K. (2025). Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare. *Cureus*, *17*(3).

[66] Zhao, J. Z., Fonseca-Sarmiento, C., & Tan, J. (2019). America's trillion-dollar repair bill. *Volcker Alliance*.

[67] Akande, S. A., & Enyejo, J. O. (2024). Leveraging predictive analytics to improve demand forecasting and inventory management in healthcare supply chains. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), Article IJSRSET2512184624. https://doi.org/10.32628/IJSRSET2512184624

[68] Akande, S. A., & Enyejo, J. O. (2023). Artificial intelligence in supply chain management: A systematic review of emerging trends and evidence in healthcare operations. International Journal of Scientific Research and Modern Technology, 3(12), 257–272. https://doi.org/10.38124/ijsrmt.v3i12.1055