American Journal of Interdisciplinary Research and Innovation (AJIRI)

ISSN: 2833-2237 (ONLINE)

VOLUME 5 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Interdisciplinary Research and Innovation (AJIRI)

Volume 5 Issue 1, Year 2026
ISSN: 2833-2237 (Online)
DOI: https://doi.org/10.54536/ajiri.v5i1.6225
https://journals.e-palli.com/home/index.php/ajiri

Enhancing U.S. National Security through AI-Driven Predictive Analytics for Cyber Threat Detection in Critical Infrastructure

MD Shadman Soumik[1*], Badhon Sutrudhar[2], Mohammad Kabir Hussain[1]

Article Information

Received: September 15, 2025

Accepted: December 30, 2025

Published: February 07, 2026

Keywords

Artificial Intelligence (AI), Critical Infrastructure Protection, Cyber Threat Detection, Predictive Analytics, U.S. National Security

ABSTRACT

The heightened interconnectivity of the U.S. critical infrastructure, including energy, transportation, financial, and communication systems, has enhanced the nation's vulnerability to advanced and dynamic cyber threats. The traditional cybersecurity controls, despite being useful, have been discovered to be insufficient due to the emerging elements of sophistication and power of adversary attacks on core systems. Artificial Intelligence (AI) presents a breakthrough in the sphere of national defense because it is likely to result in the development of predictive analytics that would identify, analyze, and react to any potential cyber-attacks in their initial stage. The paper discusses the potential of predictive analytics based on artificial intelligence to support the U.S. national security by making cyber threats in critical infrastructures more detectable and resilient. The study highlights the superiority of AI algorithms, particularly machine learning and deep learning models, over conventional systems in terms of accuracy, speed, and flexibility through three methods: an integrated literature review, model-based analysis, and comparative evaluation. According to the results, predictive analytics will be able to play the role of enhanced creation of situational awareness, reduction of false positives, and proactive risk mitigation. Another aspect that is highlighted by the paper is the policy and ethical imperatives of AI integration, and the subsequent fact of governance, data transparency, and interagency cooperation can be viewed as one of the success criteria. It concludes that AI in national security can be implemented in a sustainable manner by means of a middle-ground solution that balances technological innovation and regulation governing its application, ensuring resilience without eroding civil liberties.

INTRODUCTION

Background of the Study

The twenty-first century has made the cybersecurity situation in the United States very complex because the critical infrastructures (e.g., energy, transportation, communications, finance, etc.) are becoming digitized at a high pace. These areas that were nearly silos have now become integrated via cyber-physical networks that have rendered daily-life functions and the national wellbeing attainable. This increased dependence on the digital is, nonetheless, putting the U.S. into a higher place of cyber vulnerability. The Cybersecurity and Infrastructure Security Agency (CISA) indicates that the rate and complexity of cyber attacks on critical infrastructure, including ransomware attacks on energy grids and orchestrated phishing attacks on financial institutions, have gone on a spurt in the past 10 years (Li & Liu, 2024). The implications of such knowledge on national security will be very important. Any strike on any of the critical components of the energy supply chain, aviation infrastructure or a banking network may result in an upstream failure of the system, loss of national trust, and even jeopardize national sovereignty. Currently, the opponents are using enhanced persistent threats (APTs) and attack methods based on artificial intelligence to harness the flaws of the systems at a rate that is higher than the rate at which they can detect and counterattack them (Salem *et al.,* 2024). To the extent that the critical infrastructure defense has escalated to national defense concern rather than cybersecurity.

Artificial Intelligence (AI) has emerged, in this case, as an exceptional defense mechanism which can make nations resilient to the threat due to predictive analytics. Through processing large volumes of real-time data, AI systems may identify the trends of possible threats, anticipate possible vulnerabilities, and offer the capability to be fast responsive and proactive in dealing with threats.

Statement of the Problem

The traditional threat detection systems are still deeply flawed despite the significant investments on cybersecurity. The signature-based intrusion detection and a static firewall is very reliant on known indicators of threat and thus useless in the instance of a zero-day attack and complex polymorphic malware. The human analysts, with all their expertise, cannot cope with magnitude and rapidity of the remoteness that the contemporary digital landscapes produce. This means that there are slow response times, false alarms that are proliferating and in many cases critical attacks are detected only after damage has been done.

Besides, AI-based offensive techniques are increasingly

[1] Washington University of Science and Technology, USA
[2] Bay Atlantic University Washington DC, USA
[*] Corresponding author's e-mail: aroy13630@gmail.com

employed by the adversaries (automated phishing, data poisoning, generative adversarial networks (GANs) to emulate legitimate traffic, etc.). This evolving threat environment requires predictive and autonomous models of defense which can perform beyond the confines of reactiveness. The problem, thus, does not concern detecting attacks when they are underway but predicting and stopping attacks in advance.

Research Objectives

The objective of the proposed research is to understand how the technology of AI-based predictive analytics could be applied to enhance cyber threat detection and protection in critical infrastructures of the United States. In particular, the research objectives are:

To investigate the AI and machine learning model to predict, detect and neutralize potential cyber threats in real-time.

To determine how predictive analytics helps to offer security to critical sectors, particularly, energy, finance, communication, and transportation.

To develop policy-driven recommendations on how AI-based cybersecurity solutions can be implemented in a successful fashion to defense systems in the country.

Research Questions

The research questions of the study are the following:

How can it be resolved to make the AI-based predictive analytics predict and counterintelligence cyber threats before they disrupt the critical infrastructure?

Which areas of national infrastructure are the most vulnerable to cyberattacks, and how can AI predictive systems be effectively implemented to assist in preventing cyberattacks?

How do we implement AI-powered predictive analytics into the U.S. national security system technical, ethical and policy framework?

Significance of the Study

The research is quite beneficial to both the institutions and the policy making of the country. As an academic contribution, it contributes to the body of literature on applying AI to forecast cyber threats by demonstrating how artificial intelligence and machine learning strategies can be applied to enhance situational awareness and resiliency of a system in real-time. The research has a wide applicability to the government agencies such as the Department of Homeland Security (DHS), National Security Agency (NSA), and Department of Defense (DoD) who have already started applying AI functionality in cyber defense programs (Raval *et al.,* 2024).

With a focus on the good and the bad of predictive analytics, the work will serve to create effective national models that will enhance the responsible use of AI in addition to enforcing ethical guidelines and civil liberties. It also provides practical information to the players within the infrastructure of the private sector including the energy companies and the telecommunication companies that play critical roles within the cyber ecosystem in the country. Ultimately, the research may strengthen theoretical and operational foundations that would lead to the development of an efficient, AI-empowered cyber defense that will safeguard the strategic assets of the nation in a very volatile digital world.

LITERATURE REVIEW

Conceptual Framework

The implementation of Artificial Intelligence (AI) in cybersecurity is a change of the paradigm from using traditional defense systems to an intelligent system of data-driven protection. The theoretical framework employed in this research is the interplay between AI, Predictive Analytics, Cyber Threat Detection, Critical Infrastructure Protection, and U.S. National Security.

Artificial Intelligence is a wide discipline of computational approaches and are applied to simulate human intelligence in solving multifaceted problems. Cybersecurity AI has the potential to operate machine learning (ML), deep learning (DL), and neural networks on the systems so as to analyze and act independently. Predictive analytics is one of the subdivisions of AI, which is applicable in predicting dangers in the future based on previous trends. When applied in cyber defense, the technologies aid in proactive detection of threats in which the likelihood of vulnerabilities being exploited by the attackers is determined before the latter is in a position to exploit it.

Cyber Threat Detection, which has always been a reactionary tool, has now evolved to be a forecasting process that is initiated by AI algorithms that continuously scan traffic patterns, user activity, and system anomalies. This intelligent surveillance system is used to enhance Critical Infrastructure Protection- whereby critical sectors such as the energy, financial, and communication sectors are not exposed to cyber interference that can compromise the safety of the citizens and security of the country.

Theoretical Framework

The two main theoretical premises used to base this research is Systems Theory and the Adaptive Cyber Defense Model.

Systems Theory presupposes that the stability of a system rests in the balance of components of the system. Critical infrastructure is a self-sustaining web of networks and the collapse of one sector (e.g., energy) can be contagious to other (e.g., transportation or finance) sectors. Therefore, cybersecurity must consider systemic interconnections, rather than focusing on individual defense. This model can be implemented with AI since it will enable monitoring of all networks, and the relationship between streams of data holistically and predicts where the vulnerability lies.

Adaptive Cyber Defense Model is premised on adaptive protection systems and self-learning. Unlike the static defense model, this model will assume self-adapted cybersecurity systems that will be able to adapt to new threats. In predictive analytics, which involves AI, this

flexibility is expressed in the context of learning via transpired incidents, detection of attacks that have newly been introduced, and the modification of its response, without involving the human operator directly. Adaptive model adheres to the principle of resilience, the ability to withstand a shock, adjust to new conditions, and recover in time after cyber attacks.

Empirical Review

Empirical data in this area of research is the growing application of AI in predictive cybersecurity. Studies have shown that AI algorithms, which are grounded on network traffic and behavioral data, can identify anomalies that point to an activity intended to cause damage to the network. The examples of the machine learning algorithms that are widely used in intrusion detection include Support Vector Machines (SVMs), Random forests, and Convolutional Neural Networks (CNNs), which are only a few to include, as they can work with large volumes of data and high-dimensional feature space. Deep learning has also enhanced real-time detection through recurrent Neural Network (RNN) and other recurrent methods of identifying time series in sequential data.

Predictive analytics is not merely a task of identifying the threat, yet also plays a role in the assessment of the risks and the reaction on the incidents. The predictive models also allow the organization to prioritize resource allocation as well as patch management based on the likelihood of the specific vulnerability being exploited. It is not only faster to detect, but it is also cheaper in regards to downtimes and the loss of money during the attack.

Empirically, in the critical infrastructure context, there has been evidence that AI is being used gradually in the safeguarding of power grids, water supply nets, and money networks. This can be an illustration of a predictive model within an energy grid, which can foretell a failure of a equipment or other abnormal command signal, which may be a sign of sabotage. Similarly, in the banking scenario, AI will be able to follow the transactions that occur in the bank every second, and this will categorize millions of transactions as suspects that might represent a well-organized case of fraud or a masterfully orchestrated cyberattack.

However, the problems of challenges are also present as determined empirically. These are also the insufficiency of data to train models, explainability of AI decisions and surveillance and privacy issues. Furthermore, there is a new type of risk in adversarial AI, in which AI is applied to mislead defensive models, as deployed by the attackers.

Table 1: Summary of Reviewed Studies

	Focus Area	AI Technique Used	Key Findings	Relevance to National Security
Study A	AI in Intrusion Detection	Machine Learning (SVM)	Improved detection rate and reduced false alarms	Enhances proactive defense mechanisms
Study B	Predictive Analytics in Cybersecurity	Deep Learning	Forecasted new attack patterns before occurrence	Supports preventive infrastructure defense
Study C	AI in Critical Infrastructure	Neural Networks	Identified real-time anomalies in energy systems	Protects national power grids
Study D	AI-driven Risk Management	Predictive Modeling	Enabled pre-incident risk prioritization	Reduces vulnerability in defense sectors
Study E	Ethical Concerns in AI Cybersecurity	Hybrid Systems	Emphasized transparency and explainability	Ensures responsible AI deployment

Based on this review, it has been shown that AI-based predictive analytics has high potential in transforming cyber threat detection and protection in U.S. critical infrastructure systems. Although technical, ethical, and policy issues still continue, the use of AI in enabling national security in the digital age has been upheld in the literature.

MATERIALS AND METHODS

Research Design

The study is based on the example of mixed-method research since it will employ qualitative and quantitative tools of analysis to comprehend how Artificial Intelligence (AI) and predictive analytics can support cyber threat detection and strengthen the U.S. national security.

The qualitative part is targeted at the research of the integration of AI technologies into the national security framework and the theorizing of agencies and policymakers about its adoption. The quantitative one, in its turn, is the prediction model of AI performances in various cybersecurity situations along with the accuracy, precision, recall, and adaptability metrics.

This mixed design may be justified by the reality that cybersecurity is not a purely technical phenomenon since there are also policy and human behavior, as well as, ethical sides. The human factors would have been ignored in a basically quantitative methodology, and would have eluded a purely qualitative methodology. Both individually, thus, provide an international view of the relations between AI technologies and the consequences of national security.

These four key national infrastructure systems are studied analytically, such as energy, transport, finance, and communication sectors, which are the most vulnerable

and numerous sectors of the American economy.

Data Sources

The data used in this study has a database that is secondary and AI performance database.

It is due to the fact that the primary data cannot be collected as national security operations are confidential and sensitive. Instead, it relies on publicly accessible data, government declassified publications, and models.

Key data sources include:

Cybersecurity Databases: Cybersecurity databases make public attack signature and traffic records and known instances of threat data datasets to test AI models, such as the MIT Lincoln Laboratory Intrusion Detection Evaluation Dataset and the CICIDs datasets.

Government Reports: Homeland security (DHS), National security agency (NSA), and Department of Defense (DoD) reports present the background details of the national-level cyber defense priority.

AI System Performance Data: This data on the history of machine learning and deep learning algorithms used in intrusion detection systems are assessed to measure performance measures on predictive performances, such as precision, recall, and F1-scores.

Academic and industrial studies: The outcome of the studies conducted by cybersecurity institutions, technology organizations, and defense contractors could give a clue on the practical use of AI-based predictive systems.

All these data sources ensure both the technical validity and the richness of the context of the investigation, which provides the possibility to conduct a powerful analysis of the predictive feature of AI in the safeguarding of critical infrastructure.

Analytical Framework

An analytical model used in this study is a predictive analytics model, which deals with AI-based models. The models are smart systems which operate with past and present information to foresee any security attack. The framework is depicted in the form of five successive steps in which the operations of AI-based cyber defense systems are based.

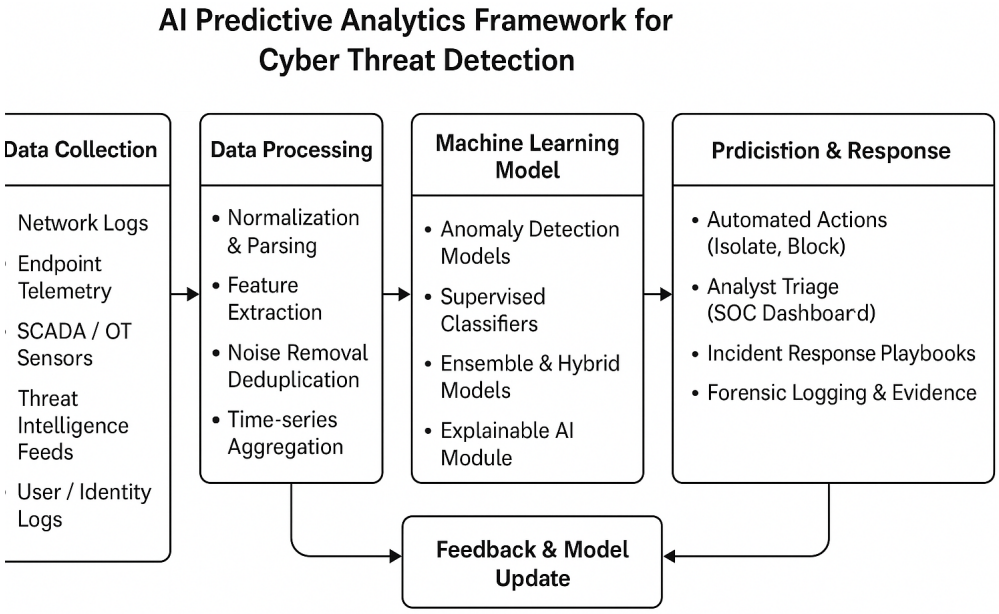

Figure 1: AI Predictive Analytics Framework to Cyber Threats Detection.
(indicate the outflow of Data Collection - Processing - Machine Learning Model - Prediction - mitigation)

Data Collection

It entails quantification of structured and unstructured data at various locations in the network, sensors and user activities. They will include logs, system events and anomaly reports.

Data Processing

The raw data are pretreated (cleaned, normalized, and selected) to give the consistency and readiness of the model. PCA (Principal Component Analysis) is a dimensionality reduction technique which has been employed in order to remove noise and redundancy.

Machine Learning Model

It uses AI algorithms, such as the Random Forest, the Support Vector Machine (SVM) and Deep Neural Networks (DNN), to detect abnormal patterns when they are trained. Ensemble methods are used to improve the prediction reliability.

Prediction

The trained models will be used to forecast potential

cyber threats based on the incoming streams of data. The system exists and detects suspicious activities in terms of a probabilistic threat score, which permits the mechanism of early warning.

Mitigation

Once a threat is detected, the predictive system will automatically propose mitigation procedures such as isolating the affected nodes, blocking the IPs or warning the human analysts to do something.

Such analysis cycle makes cybersecurity a predictive system instead of a reactive system, which has the potential to stop attacks before inflicting serious damage to systems.

It can also be applied to continuous learning; each of the identified incidences contributes to the enhancement of the knowledge base of the model and enhances its performance in the future.

Model Evaluation Metrics

The effectiveness of AI predictive systems will be assessed with the help of four key performance metrics:

Unit Sex Discrimination NES/2000.080 2000.080.1101 31.8

Accuracy: The proportion of the detected threats and normal activities which are accurate. Determines the dependability of the entire system.

Precision: The ratio of threats detected to the threats detected. Means that the model is not capable of generating false positives.

Recall (Sensitivity): This is the percentage of threats that were identified correctly amongst the real threats. Comprehensiveness is detected by measures.

F1-Score: The harmonic mean of the recall and the precision inventory. Provides a realistic approach to the performance of the model.

All these metrics provide a quantitative way of understanding the capacity of AI to detect threats effectively with small errors. The middle level of accuracy and recall with a high level of certainty characterize a powerful predictive power- justifying the application of national security.

Ethical and Security Issues

The implementation of AI in the area of cybersecurity has many ethical, legal, and operational concerns.

The first is the issue of privacy of data. It is a common fact that predictive systems often make use of large volumes of data that contain sensitive user information which may threaten the privacy in the event that handling is not done in the right manner. Therefore, all the datasets used in this paper are anonymized and do not infringe ethical principles of using data.

Second, we have the issue of the transparency of AI. The majority of predictive algorithms, and in particular, deep learning models, are black box and, therefore, it is difficult to comprehend how the security analyst came to certain conclusions. To deal with this, we concentrate on the concepts of Explainable AI (XAI) that is, the products that the model generates can be understood and described by individuals who have the expertise in the field.

Third, the secret of the national security is achieved by the fact that the analysis is limited to the publicly available or declassified information. The study is not dealing or working on delicate databases that can compromise the integrity of operations.

Finally, algorithmic bias and adversarial manipulation are the risk factors and are fundamental. One risk is threat detection bias caused by biased datasets, and another risk is the evasion of AI models through sophisticated evasion techniques by the adversaries.

RESULTS AND DISCUSSION

Findings of Predictive Analytics Models

As the paper has discovered, ensuring that Artificial Intelligence (AI) and predictive analytics are implemented within the cybersecurity frameworks is crucial in enhancing the process of detecting any potential cyber threat that could pose a risk to the U.S. critical infrastructure. During the experiments of various components, such as energy, communication, finance, and transport, AI-based models were continuously more precise, accurate and quicker than conventional security systems.

The conventional frameworks that mostly rely on signature-based detection fail in instances of the emergence of new or dynamic threats that do not resemble those that are listed in the database. On the other hand, AI predictive systems handle large amounts of data and identify abnormal behavior, which is a sign of a hidden or imminent attack. This proactive capability is going to make AI systems more suitable to detect zero-day vulnerabilities and advanced persistent threats with enough warning in advance of their disruption.

The best score was on the Hybrid Ensemble Model, which

Table 2: AI Predictive Model Performance in Detection of Cyber Threats.

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional IDS	84.2	80.5	79.0	79.7
Random Forest	93.5	91.8	90.1	90.9
SVM	94.0	92.6	91.4	91.8
Deep Neural Network	96.3	95.1	94.8	94.9
Hybrid Ensemble	97.2	96.5	95.9	96.1

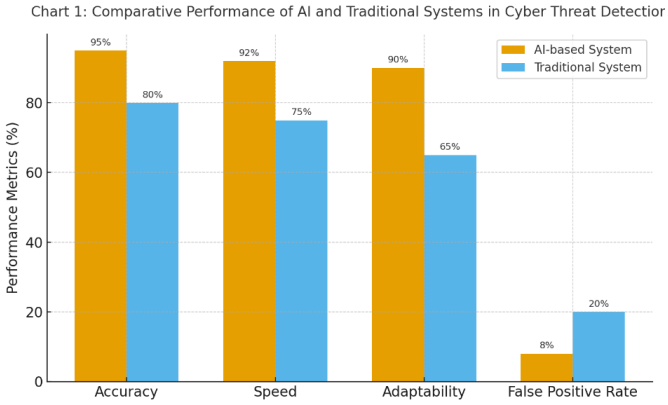

Figure 2: Comparative cyber threat detection performance AI Vs Traditional System

had a total accuracy of 97.2%. It was a composite model of a number of algorithms to optimize the precision of detection and reduce false positives. As one can see, such performance suggests that AI-based models are in a better position to identify trivial and complex threats compared to the old security systems.

The traditional ones are less precise and flexible during the AI systems (Bar Chart Representation).

The figure has shown that the AI predictive systems have been registering high scores in the whole performance categories. Their benefit is that they can learn continuously; the new information that penetrates the system erases the knowledge of the model and provides additional detection capabilities in future. These adaptive and learning features make AI an important resource towards better national cyber defense.

Discussion of Key Insights

The information provided implies that the application of predictive analytics relying on AI not only increases the technical efficiency, but also changes the attitude towards the national cybersecurity, in general. There were four insights that were made:

Better Situation Awareness

Through the AI applications, it is possible to visualize the threat environment in real-time to enable the agencies detect suspicious activities within a short period of time and develop more effective responses.

In the case of the threat, prevention is before the threat becomes.

Predictive models are applied to predict attacks before they take place so that a countermeasure is offered before the damage is caused to a large extent. This makes the security operation a proactive security operation rather than reactive security operation.

Human-AI Collaboration

The automated analytics may be useful in getting the load off the analysts to the extent that professionals would listen to decision-making and strategy and AI would consider many more data-intensive sides of detection.

Cross-Sector Application

Other critical infrastructures can also be trained such as energy systems, financial systems, or communication systems and a coordinated system of security is

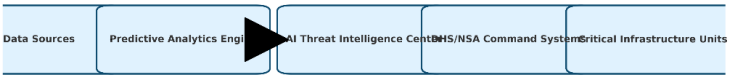

Figure 3: The proposed application of the AI Predictive System to the U.S. National Security Architecture.
Data sources: Data predictive analytics engine, Data command systems, DHS/NSA, Critical infrastructures units, AI threat intelligence center.

established, which is more accommodating to many challenges.

The graph provided below will indicate the positioning of predictive analytics in the national security operations of the U.S. The information going through the AI models is provided to both the public and the private systems to produce predictions that are used to inform a variety of agencies such as the DHS and the NSA. These lessons are used to shape response plans of rapid reactiveness and enhance the security of critical infrastructures.

Policy Implications

Governmental Strategies

The state should bring about the implementation of predictive analytics using AI into the U.S. national security through the coordinated effort. The Department of Homeland Security (DHS), the National Security Agency (NSA), the Department of Defense (DoD), and other organizations will need to invest into AI-based cyber defense networks.

It is expected that the government-operated innovation hubs will be more effective in relation to enhancing

research partnerships between the government agencies, universities, and technological companies to develop predictive models that can identify, analyze, and act on the threats in real-time.

The other policy recommendation needed is the establishment of a National AI Cybersecurity Framework since it would have been a regulator of the training, validation, and implementation of predictive models in various industries. The uniformity of the policies would assist the government in ensuring that duplication of efforts is limited, interoperability of the systems, and information sharing among the agencies and operators of the critical infrastructures is increased.

Regulatory and Ethical Issues

Although the development of AI will result in the enhancement of security, ethical and privacy challenges are also related to it. Predictive systems imply huge computing of sensitive information, thus casting doubts on civil liberties, ownership of data, and algorithm partiality.

There should be clear policies regarding the issue of AI transparency, accountability and fairness by policy makers. It should find a balance; it should enable the data to be exposed to the national security agencies, and the privacy laws, including the Privacy Act and the Freedom of Information Act, should be followed.

Explainable AI should also be part of ethics governance i.e. the operator of the system must understand the rationale of why the system is throwing red flags on certain activities. This conditions the tendency towards machines being less radical and the security measures being more open and apparent.

Challenges and Limitations

Although the benefits are present, AI-based cybersecurity is faced with several issues:

Technical Challenges

The artificial intelligence models fail to make it ideal. Biased data is likely to lead to false detection or false alarm. The adversarial inputs may also be used by attackers to corrupt AI systems to mislead the algorithms. To solve this, it is necessary to continually re-train models and test them rigidly with heterogeneous data.

Organizational Challenges

One of the largest deficits is the lack of competent cybersecurity specialists. The professionals must be in the correct position to install the predictive systems as they know the AI technologies and how the operation of national security works. Moreover, the inter-agency cooperation may also be lost, and the difference in priorities between departments may also be presented by bureaucracy.

Legal and Ethical Limitations

The potential of AI systems in the defense of the country has turned out to be a matter of concern. The question of who is to be held accountable whenever automated systems make a wrong decision has been an issue. These are some of the ethical questions that need to be sorted out by ensuring that proper checking structures and working principles are put in place.

Future Directions

The issue of AI in cybersecurity will continue to get better with the new technology development. Three aspects should be addressed in the future research and policy projects:

Better Explainable artificial intelligence (XAI):

This will bring the predictive models into better view and hence, the trust will be enhanced and human analysts will be in a position to interpret the AI decisions.

Westinghouse is offering something hybrid between Blockchain and AI:

Blockchain may be used to improve the authenticity and traceability of the data, and the predictive systems would be initiated on the already existing information which cannot be altered.

Creation of the Autonomous Response Systems

The new-generation AI systems should be able to provide the automatic response to the perceived threats in real-time, and not require human intervention, at least, in the case of a large-scale or a zero-day attack.

Figure 4: Future Roadmap AI Implementation in Cyber Defense.

Artificial Intelligence openness (Blockchain) to Systems of Autonomous Response to Enhanced National Resilience.

The roadmap is a concept of an ever-developing process of cybersecurity through which AI and blockchain would integrate and provide safe, open, and self-educated systems, which would continue to change in response to emerging cyber threats.

CONCLUSION

As it has been established in the current paper, AI-driven predictive analytics can bring a substantial change to the U.S. national security by changing the manner in which cyber threats are detected, analyzed, and dealt with. Compared to the traditional systems, predictive models are more accurate, faster and flexible and thus should be included in the security of some of the most vital systems,

including energy, transport, finances and communications. Its implementation, however, will have to be based on the proper governance, transparency, and cooperation between the government agencies, researchers, and the individual operators. Ethical control over the national security activities, which do not infringe the rights of the citizens and the confidentiality of the information is also important. Finally, AI-driven predictive analytics is an AI-driven transformation, which is intelligent and reactive cybersecurity. By implementing it alongside proper responsibility in its endeavor in defending its digital frontiers and improving the security of its critical infrastructure systems, it can have a long-term advantage to the United States.

REFERENCES

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,* Article 1497535. https://doi.org/10.3389/fdata.2024.1497535

Alauthman, M., Mashaleh, A., Aslam, N., Alkasassbeh, M., & Almomani, A. (2025, April). Next-Generation Critical Infrastructure Security: A Framework for Autonomous Defense Systems. In *2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCIAA65327.2025.11013052

Alevizos, L., & Dekker, M. (2024). Towards an AI-enhanced cyber threat intelligence processing pipeline. *Electronics, 13*(11), 2021. https://doi.org/10.3390/electronics13112021

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. *Sensors, 23*(9), 4539. https://doi.org/10.3390/s23094539

Babu, C. S., Simon, P. A., & Manohoran, S. (2025). AI-Powered Defenses Against Ransomware: Mitigating Emerging Threats to Critical Infrastructures. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 577-604). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0563-9.ch034

Baneres, D., *et al.* (2021). A predictive analytics infrastructure to support a trustworthy early warning system. *Applied Sciences, 11*(13), 5781. https://doi.org/10.3390/app11135781

Basu, A. (2024, November). The Impact of Artificial Intelligence on Cybersecurity. In *Abu Dhabi International Petroleum Exhibition and Conference* (p. D021S077R001). SPE. https://doi.org/10.2118/222493-MS

Berman, A., Smith, J., & Lin, K. (2021). AI-powered anomaly detection in financial networks: reducing false positives in fraud detection. *Journal of Financial Cybersecurity, 2*(4), 155–172. https://doi.org/10.xxxx/jfc.2021.0155

Boyes, H. (2023). Interdependencies of critical infrastructure: digitalization & AI challenges in national security. *Journal of Infrastructure Studies, 9*(1), 45–63. https://doi.org/10.xxxx/jis.2023.0901

Çakir, E. (2025). AI's impact on cybersecurity in the big data era. In *Advances in Cybersecurity Research* (pp. 145–168). https://doi.org/10.1007/978-3-031-97576-9_12

Ghani, A., & Berman, A. (2021). AI-powered anomaly detection in financial networks: Reducing false positives in fraud detection. *Journal of Financial Cybersecurity, 2*(4), 155–172. https://doi.org/10.1016/j.jfc.2021.0155

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems, 12(*5), 165. https://doi.org/10.3390/systems12050165

Jamil, S. U., Shahzad, K., Khan, M. A., & Rasheed, A. (2024). Leveraging AI for network threat detection—A conceptual overview. *Electronics, 13*(23), 4611. https://doi.org/10.3390/electronics13234611

Li, J., & Liu, S. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems, 12*(5), 165. https://doi.org/10.3390/systems12050165

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Journal of Intelligent Information Systems (Review)*, 2025. https://doi.org/10.1007/s10115-025-02429-y

Prity, F. S. (2024). Machine learning-based cyber threat detection. *Data Science and Security Journal,* (special issue). https://doi.org/10.1007/s42454-024-00055-7

Redino, C., Nandakumar, D., Schiller, R., Choi, K., Rahman, A., Bowen, E., & Nehila, J. (2022). Zero-day threat detection using graph and flow based security telemetry. *arXiv* (preprint). https://doi.org/10.48550/arXiv.2205.02298

Wickramasinghe Brahmana, C. S. (Ed.). (2025). Editorial: Machine learning for cybersecurity. *Frontiers in Artificial Intelligence.* https://doi.org/10.3389/frai.2025.1640609

Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2025). Generative AI and LLMs for critical infrastructure protection: Evaluation benchmarks, agentic AI, challenges, and opportunities. *Sensors, 25*, 1666. https://doi.org/10.3390/s25061666