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)

Check for updates

Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review

Adebunmi Okechukwu Adewusi [1], Ugochukwu Ikechukwu Okoli [2], Temidayo Olorunsogo [3], Ejuma Adaga [4], Donald Obinna Daraojimba [5,*] and Ogugua Chimezie Obi [6]

[1] *University of Ilorin, Nigeria.*
[2] *Independent Researcher, Manchester, UK.*
[3] *Independent Researcher, Colorado, USA.*
[4] *Independent Researcher, Illinois, USA.*
[5] *Department of Information Management, Ahmadu Bello University, Zaria, Nigeria.*
[6] *Independent Researcher, Lagos, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 21(01), 2263–2275

Publication history: Received on 16 December 2023; revised on 23 January 2024; accepted on 25 January 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.1.0313

Abstract

Artificial Intelligence (AI) has emerged as a transformative force in the field of cybersecurity, playing a pivotal role in safeguarding national infrastructure. This review focuses on the application of AI technologies within the context of the United States, examining their efficacy in fortifying critical systems against evolving cyber threats. The paper delves into various AI-driven cybersecurity strategies, ranging from anomaly detection and predictive analysis to threat intelligence and automated response mechanisms. The integration of AI in cybersecurity not only enhances the speed and accuracy of threat detection but also addresses the dynamic nature of cyber threats. The specific AI technologies employed in the United States, including machine learning, natural language processing, and neural networks, highlighting their contributions to bolstering the resilience of national infrastructure are also examined. Furthermore, the challenges and ethical considerations associated with the widespread adoption of AI in cybersecurity are assessed. It discusses the need for robust regulatory frameworks to govern the deployment of AI in sensitive domains and emphasizes the importance of collaboration between government agencies, private enterprises, and research institutions to foster innovation and address emerging threats. In conclusion, this review provides a comprehensive analysis of the role of AI in cybersecurity within the United States, emphasizing its significance in protecting critical national infrastructure. By exploring technological advancements, challenges, and ethical considerations, this paper contributes to the ongoing discourse on leveraging AI to safeguard against the ever-evolving landscape of cyber threats.

Keywords: Artificial Intelligence; Cybersecurity; National Infrastructure; USA; Review

1. Introduction

The ever-expanding digital landscape, coupled with the increasing sophistication of cyber threats, has prompted nations to explore advanced technologies to safeguard critical infrastructure. In the United States, the integration of Artificial Intelligence (AI) into cybersecurity has emerged as a pivotal strategy to fortify the nation's resilience against cyber threats and protect its critical infrastructure (de Azambuja et al., 2023, Abbas et al., 2019). This comprehensive review aims to delve into the multifaceted realm of AI in cybersecurity, with a specific focus on its role in safeguarding the national infrastructure of the United States.

* Corresponding author: Donald Obinna Daraojimba

As a global economic and technological powerhouse, the United States faces a myriad of cyber threats that target essential sectors, including energy, finance, healthcare, and transportation (Solar, 2023, Bobish, 2023). The complexity and scale of these threats necessitate innovative solutions, and AI has emerged as a game-changing technology capable of enhancing detection, response, and mitigation capabilities in the realm of cybersecurity (Rich, 2023).

Artificial intelligence (AI) is increasingly being used to enhance cybersecurity (Kumar et al., 2023, Bharadiya, 2023, Turgay, 2023). IBM Security provides transformative, AI-powered solutions that optimize analysts' time—by accelerating threat detection, expediting responses, and protecting user identity and datasets—while keeping cybersecurity teams in the loop and in charge (Lemieux, 2023, Heilig, and Scheer, 2023). BlackBerry also offers AI-powered cybersecurity solutions that enhance protection by using artificial intelligence and machine learning (Roba et al., 2023, Tuteja, and Marwaha, 2023). AI is less error-prone and more efficient than human analysts (Srinivasan et al., 2023). While humans will always be part of the cybersecurity equation, many processes related to network security can be automated and handled by AI, reducing input errors, speeding up security-related processes, and increasing the SOC's ability to detect unknown threats. However, AI can also be a double-edged sword. It can be a powerful tool to combat cyber threats, but it can also be a dangerous cybersecurity risk. Therefore, it is important to harness AI responsibly and securely.

Kaur, Gabrijelčič, and Klobučar (2023) did a literature review and gave a future research direction on artificial intelligence for cybersecurity. Artificial intelligence (AI) is a potent technology that cybersecurity teams may use to better the security posture against a variety of security challenges and cyberattacks. AI enables these teams automate repetitive processes, faster threat detection and response, and improve the accuracy of their actions. This paper provides a thorough study of AI use cases for cybersecurity provisioning together with a methodical evaluation of the literature. 2395 studies were found in the review, 236 of which were classified as primary. This article uses a thematic analysis approach to classify the found AI use cases based on a NIST cybersecurity framework. Consumers will receive a thorough understanding of the ways in which artificial intelligence (AI) might enhance cybersecurity in various settings from this classification structure. In order for AI-based cybersecurity to be successfully adopted in the current era of digital transformation and polycrisis, the assessment also outlines future research possibilities in data representation, advanced AI methodologies, rising cybersecurity application fields, and the creation of new infrastructures.

By conducting a thorough review of the current state of AI in cybersecurity in the United States, this comprehensive analysis aims to provide valuable insights that can inform strategic decisions and policy development. The goal is to contribute to the ongoing efforts to fortify the nation's cybersecurity defenses, safeguard critical infrastructure, and ensure the resilience of the United States in the face of emerging cyber threats.

2. Background and significance of AI in cybersecurity

The ever-evolving landscape of cyber threats necessitates constant innovation and adaptation within cybersecurity (Safitra, Lubis, and Fakhrurroja, 2023). Artificial intelligence (AI) has emerged as a powerful tool, offering significant potential to enhance security posture and mitigate cyber risks (Chakraborty, Biswas, and Khan, 2023, Djenna et al., 2023, Sanni et al., 2024). AI in cybersecurity is the application of artificial intelligence (AI) technologies to protect online systems and data from cyberattacks and unauthorized access. AI in cybersecurity is significant because it can help automate and enhance the detection, prevention, and response of cyber threats, as well as reduce the human error and resource constraints that often challenge traditional security methods (Sufi, 2023). Some of the benefits of AI in cybersecurity are here presented. AI can analyze large and complex data sets to identify patterns, anomalies, and vulnerabilities that may indicate malicious activities or potential risks (Mishra, 2023). AI can learn from previous data and experiences to adapt to new and evolving threats, as well as generate proactive and predictive solutions. AI can automate tedious and repetitive tasks, such as system monitoring, malware scanning, and incident reporting, and free up human resources for more strategic and creative activities (Uzoma et al., 2023). AI can enhance the accuracy, efficiency, and speed of security operations, as well as reduce the costs and time associated with security breaches.

AI in cybersecurity is not a new concept, but it has gained more attention and importance in recent years due to the increasing sophistication and frequency of cyberattacks, as well as the growing volume and diversity of data and devices that need to be secured. AI in cybersecurity is also influenced by the development and adoption of other emerging technologies, such as cloud computing, blockchain, IoT, and 5G, which create new opportunities and challenges for security. Therefore, AI in cybersecurity is a dynamic and evolving field that requires continuous research, innovation, and collaboration among various stakeholders, such as governments, industry, academia, and civil society.

Initial applications of AI in cybersecurity focused on anomaly detection and intrusion prevention systems. This represents the early stages (1990s-2000s). Machine learning era starts from 2010s-present. The rise of machine learning algorithms revolutionized AI-powered cybersecurity solutions, enabling more sophisticated threat identification, analysis, and prediction. There come the deep learning advancements from 2020s-present. Deep learning techniques further enhance AI capabilities, allowing for more nuanced and complex threat analysis, including recognizing zero-day attacks and identifying hidden patterns in cyberattacks.

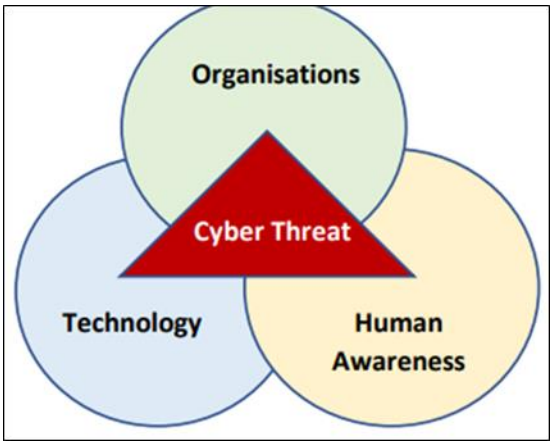

Figure 1 Small and medium scale enterprise categories to mitigate cyber threats (Rawindaran, 2023)

Figure 1 shows the approached employed my small and medium scale enterprise to mitigate cyber threats and attacks.

AI algorithms analyze vast amounts of data from diverse sources, enabling proactive identification of even the most subtle threats. AI systems can automate incident response processes, including containment, remediation, and recovery, significantly reducing response times. AI models analyze historical data and current trends to predict future cyberattacks, enabling proactive mitigation strategies and resource allocation. AI systems can personalize security solutions to specific environments and threats, enhancing their effectiveness and efficiency. AI can address the growing gap in cybersecurity talent by automating routine tasks and augmenting human expertise.

2.1. AI Application in Cybersecurity

The specific applications of AI in cybersecurity are here presented. AI in cybersecurity is the use of artificial intelligence technologies to protect online systems and data from cyberattacks and unauthorized access. AI can analyze large and complex data sets to identify patterns, anomalies, and vulnerabilities that may indicate malicious activities or potential risks. AI can also learn from previous data and experiences to adapt to new and evolving threats, and generate proactive and predictive solutions. AI can integrate and synthesize information from various sources, such as threat intelligence feeds, security logs, and network traffic, to provide a comprehensive and holistic view of the security situation. AI can also help prioritize and correlate the most relevant and critical data for security analysts. AI can help discover and mitigate the thousands of cyber events that organizations encounter daily, by using techniques such as behavioral analytics, natural language processing, and image recognition. AI can also help differentiate between the actions of authorized users and good bots versus unauthorized users and malicious bots. AI can help assess the likelihood and impact of a security breach, by using data analytics, machine learning, and simulation models. AI can also help identify and address the root causes and vulnerabilities that may lead to a breach, and suggest mitigation actions. AI can help automate tedious and repetitive tasks, such as system monitoring, malware scanning, and incident reporting, and free up human resources for more strategic and creative activities. AI can also help automate the response and remediation of security incidents, by using predefined rules, policies, and workflows.

Figure 2 Major cybersecurity challenges faced by financial institutions (Kayode-Ajala, 2023)

Phising is among the key cybersecurity found in various sector especially the financial institutions as shown in figure 2.

These are some of the specific applications of AI in cybersecurity, but they are not the only ones. AI can offer many benefits and opportunities for improving the security of online systems and data, but it also poses some challenges and risks, such as data quality, privacy, security, ethics, and governance. Therefore, it is important to ensure that AI is developed and used in a responsible, transparent, and inclusive manner, with respect for human rights and security standards.

Identifying and classifying malware using AI algorithms based on behavior, code patterns, and network activity (Majid et al., 2023, Moorthy, and Nathiya, 2023). Recognizing and filtering phishing emails through AI analysis of text, links, and sender information. Prioritizing and patching vulnerabilities based on AI-driven risk assessments and exploit prediction. Identifying anomalous user behavior and potential insider threats through AI-powered monitoring and analysis (Islam, 2023). Tracing the origin of cyberattacks through AI-powered analysis of network activity and digital footprints.

2.1.1. Challenges and considerations

AI systems rely on vast amounts of data, raising concerns about data privacy and security. AI algorithms may perpetuate existing biases, leading to discriminatory outcomes in cyber threat detection and mitigation. AI models can be complex and opaque, hindering accountability and trust in their decisions. Cybercriminals may develop techniques to manipulate AI systems, leading to false positives or negatives.

AI in cybersecurity is the application of artificial intelligence technologies to protect online systems and data from cyberattacks and unauthorized access. The future of AI in cybersecurity may involve the following trends and developments. As AI becomes more accessible and powerful, cybercriminals may use it to create more sophisticated and stealthy attacks, such as generating fake content, impersonating users, bypassing security measures, and exploiting vulnerabilities. Therefore, security professionals need to be prepared to defend against AI-enabled threats, as well as to leverage AI for their own advantage. As cyberattacks become more complex and frequent, security solutions need to be more intelligent and adaptive. AI can help automate and enhance the detection, prevention, and response of cyber

threats, as well as reduce the human error and resource constraints that often challenge traditional security methods. AI can also help integrate and synthesize information from various sources, such as threat intelligence feeds, security logs, and network traffic, to provide a comprehensive and holistic view of the security situation. As AI plays a more prominent role in cybersecurity, it also raises ethical and governance issues, such as data quality, privacy, security, accountability, and transparency. AI in cybersecurity needs to be developed and used in a responsible, transparent, and inclusive manner, with respect for human rights and security standards. AI in cybersecurity also needs to be regulated and supervised by appropriate authorities and stakeholders, such as governments, industry, academia, and civil society.

Table 1 Existing Governance in UK (Post Brexit) and EU (Rawindaran, 2023)

Governance	Abbreviation	UK	EU
General Data Protection Act	GDPR	X	X
Digital Services Act	DSA	-	X
Online Safety Bill	OSB	X	X
Digital Marketing Act	DMA	-	X
Data Protection Act	DPA	X	-
ISO27001	ISO27001	X	X
Cyber Essentials + Plus	CE/CEP	X	-

As shown in table 1, the identity with the General Data Protection Regulation (EU) 2016/679 (GDPR). As one of the most wide-ranging pieces of EU legislation across the single market, GDPR was introduced to standardise data protection laws to give greater control over personal data and how it is used in a growing digital economy. Although originally passed in the EU, the principles-based approaches affect businesses worldwide and includes fairness, lawfulness and transparency, purpose limitation, data minimalization, accuracy, storage limitation, integrity, and confidentiality (security), and accountability (Rawindaran, 2023)

These are some of the possible aspects of the future of AI in cybersecurity, but they are not the only ones. AI in cybersecurity is a dynamic and evolving field that requires continuous research, innovation, and collaboration among various stakeholders, as well as the integration of scientific evidence, policy frameworks, and best practices.

Despite challenges, the future of AI in cybersecurity is promising. Continued research and development will lead to even more advanced and effective solutions, helping organizations stay ahead of evolving cyber threats and protect their critical assets.

2.1.2. Overview of the role of AI in protecting national infrastructure

Artificial intelligence, is the technology that enables machines to perform tasks that require human intelligence, such as learning, reasoning, and decision making. AI can play an important role in protecting national infrastructure, which refers to the systems and assets that are essential for the functioning and security of a nation, such as transportation, energy, communication, and water.

AI can help detect and prevent cyberattacks on critical infrastructure, by using data analytics, machine learning, and natural language processing to identify patterns, anomalies, and vulnerabilities that may indicate malicious activities or potential risks. AI can also help automate and enhance the response and remediation of security incidents, by using predefined rules, policies, and workflows. AI can help optimize the performance and resilience of critical infrastructure, by using sensors, computer vision, and deep learning to monitor and control the physical and digital components of the infrastructure, such as power grids, pipelines, and traffic lights. AI can also help predict and mitigate the impacts of natural and man-made disasters, such as earthquakes, floods, and fires, on the infrastructure. AI can help innovate and transform critical infrastructure, by using data mining, pattern recognition, and image recognition to discover and

exploit new opportunities and challenges for the infrastructure, such as renewable energy sources, smart cities, and IoT devices. AI can also help enhance the user experience and satisfaction of the infrastructure, such as by providing personalized services, feedback, and recommendations.

These are some of the ways that AI can help protect national infrastructure, but they are not the only ones. AI can offer many benefits and opportunities for improving the security, efficiency, and sustainability of national infrastructure, but it also poses some challenges and risks, such as data quality, privacy, security, ethics, and governance. Therefore, it is important to ensure that AI is developed and used in a responsible, transparent, and inclusive manner, with respect for human rights and infrastructure standards.

National infrastructure is the backbone of modern society, encompassing critical systems like energy grids, transportation networks, communication systems, and water treatment facilities. Protecting this infrastructure from cyberattacks and other threats is essential for national security, economic prosperity, and public safety. Artificial intelligence (AI) is emerging as a powerful tool for enhancing the security and resilience of national infrastructure, offering significant potential in various aspects. AI algorithms analyze vast amounts of data from sensors, cameras, and network traffic, identifying anomalies and potential threats that might escape human detection. Machine learning models can learn and adapt to evolving threats, detecting zero-day attacks and identifying subtle patterns that indicate malicious activity. AI-powered threat intelligence platforms collect and analyze threat data from diverse sources, providing comprehensive situational awareness to security teams. AI can predict potential equipment failures and infrastructure vulnerabilities before they occur, enabling preventive maintenance and reducing downtime. AI-powered risk assessment models analyze various factors like weather conditions, traffic patterns, and historical data to identify areas most susceptible to disruptions. Predictive analytics enable resource allocation and response planning to mitigate risks and minimize potential damage from incidents.

AI systems can automate various aspects of incident response, including isolating affected systems, containing threats, and restoring operations quickly. AI-powered decision support tools help security teams prioritize responses, optimize resource allocation, and minimize disruption during cyberattacks. Self-healing infrastructure systems can automatically detect and repair minor issues, reducing reliance on human intervention and improving resilience.

AI-powered intrusion detection systems can identify and prevent unauthorized access attempts, protecting critical systems from cyberattacks. Behavioral analysis algorithms can detect anomalous user activity and identify potential insider threats. AI-based authentication and authorization systems can provide more secure and efficient access control to sensitive infrastructure components.

2.1.3. Benefits of AI for National Infrastructure Protection

AI helps identify and mitigate threats more effectively, reducing the risk of disruptions and ensuring the reliability of critical infrastructure (Halim et al., 2023, Štitilis, Laurinaitis, and Verenius, 2023). AI-powered predictive maintenance and automated responses optimize resource usage and minimize downtime, leading to cost savings and increased efficiency (Pinto et al., 2023). AI helps build more resilient infrastructure by predicting and preventing failures, enabling rapid recovery from disruptions, and adapting to evolving threats. AI provides data-driven insights to inform decision-making, enabling proactive risk management and effective resource allocation. Reduced reliance on human expertise. AI can automate tasks and augment human capabilities, addressing the cybersecurity workforce shortage and improving overall response effectiveness.

2.1.4. Challenges and Considerations

AI systems require vast amounts of data, raising concerns about data privacy and security. Robust data governance frameworks are essential. AI algorithms may perpetuate existing biases, leading to discriminatory outcomes in threat detection and resource allocation. Mitigating bias is crucial. AI models can be complex and opaque, hindering accountability and trust. Transparent AI solutions are necessary. Cybersecurity of AI systems. AI systems themselves are susceptible to cyberattacks, requiring robust security measures to protect them from manipulation. Utilizing AI for national infrastructure protection raises ethical considerations regarding data privacy, use of surveillance technology, and potential for bias in decision-making.

AI offers tremendous potential for enhancing the security and resilience of national infrastructure. By addressing challenges and implementing AI responsibly, we can leverage this powerful technology to safeguard critical systems, ensure public safety, and build a more secure and prosperous future for all.

2.2. AI Technologies in Cybersecurity

AI technologies play a crucial role in enhancing cybersecurity measures, providing advanced capabilities to detect, prevent, and respond to evolving cyber threats. Some key AI technologies used in cybersecurity are represented in the figure 3.

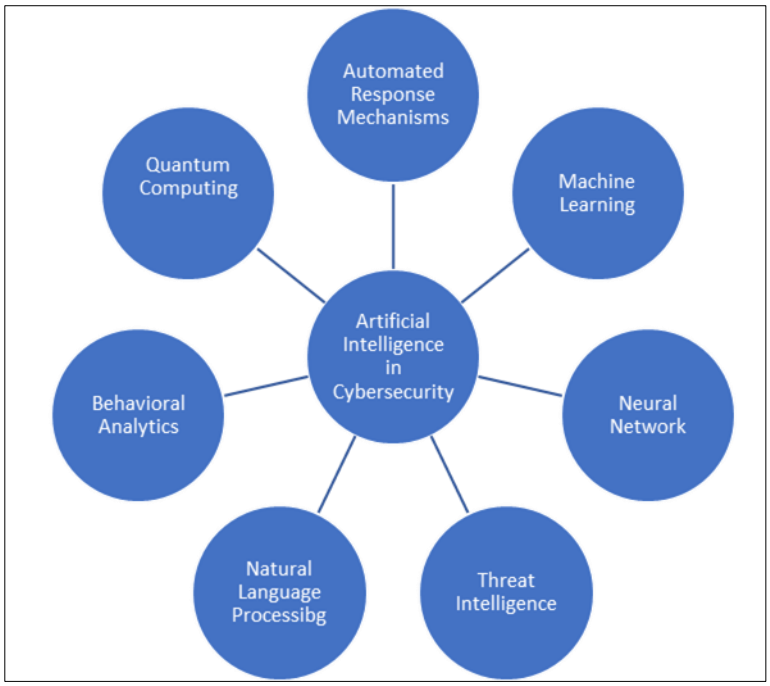

Figure 3 Key technologies of Artificial Intelligence in Cybersecurity

Some of the key technologies of AI used in cybersecurity include machine learning, threat intelligence, neural network, behavioural analytics, quantum computing (Sarker, 2023, Khang et al., 2023). Machine Learning (ML) algorithms analyze normal behavior patterns and identify anomalies that may indicate potential security threats. ML models predict and assess potential future cyber threats based on historical data, helping organizations proactively strengthen their defenses. Natural Language Processing (NLP) processes and understands human language, aiding in the analysis of vast amounts of textual data to identify security-related information. NLP facilitates improved communication and collaboration among security systems by interpreting and contextualizing human-generated data and reports. Neural networks, a subset of machine learning, enable deep learning techniques for complex pattern recognition in large datasets, enhancing the accuracy of threat detection. Neural networks are particularly effective in identifying sophisticated and evolving cyber threats by learning and adapting to new patterns. AI processes vast amounts of data to extract relevant threat intelligence, enabling organizations to stay informed about the latest cyber threats. AI systems continuously monitor and analyze data in real-time to identify and respond to emerging threats promptly. AI-driven automation accelerates incident response times by automating routine tasks, allowing cybersecurity teams to focus on more complex and strategic aspects of threat mitigation. AI enables security systems to adapt and evolve in response to changing threat landscapes, ensuring that defense mechanisms remain effective against new and emerging threats.

AI analyzes user behavior and entity interactions to detect deviations from normal patterns, helping identify potential insider threats or compromised accounts. Behavioral analytics, powered by AI, provides continuous monitoring of network activities, improving the detection of abnormal behaviors indicative of security incidents. With the advent of quantum computing, AI is utilized to develop and implement cryptographic algorithms that can withstand quantum attacks, ensuring the security of sensitive data in the post-quantum era.

AI technologies in cybersecurity are dynamic and continue to evolve, adapting to new challenges and threats. The integration of these technologies enhances the overall resilience of cybersecurity measures, allowing organizations to proactively address and mitigate potential risks.

2.3. AI Strategies for National Infrastructure Protection

AI strategies play a pivotal role in safeguarding national infrastructure, providing advanced capabilities for threat detection, response, and overall cybersecurity resilience (Xia, Semirumi, and Rezaei, 2023). Some key AI strategies employed for national infrastructure protection are here discussed. AI analyzes large datasets to identify and assess potential threats in real-time, providing rapid insights into emerging risks. AI models leverage historical data to predict and anticipate future cyber threats, allowing proactive mitigation strategies (Khonturaev, Khoitkulov, and Abdullayeva, 2023). AI-driven automation accelerates incident response times by automating routine tasks, allowing for swift identification, containment, and eradication of cyber threats. AI facilitates the orchestration and coordination of incident response processes across multiple security tools and platforms. AI analyzes user and entity behaviors to detect anomalies and potential insider threats, enhancing the security posture by identifying unusual activities. UEBA powered by AI provides continuous monitoring of user activities, helping identify deviations from normal behavior. Intrusion Detection and Prevention Systems (IDPS). AI enhances IDPS capabilities by quickly identifying and responding to network intrusions, minimizing the impact of cyber attacks. AI analyzes network traffic patterns to detect unusual activities, enabling the identification of potential threats and vulnerabilities.

AI monitors and analyzes endpoint behaviors to identify and prevent malicious activities at the device level. Endpoint Detection and Response (EDR). AI-driven EDR solutions provide real-time visibility into endpoint activities, enabling rapid response to security incidents. AI processes and analyzes large volumes of security data to identify patterns, trends, and potential security incidents that may go unnoticed by traditional methods. Correlation of Threat Indicators. AI correlates various threat indicators to provide a holistic view of cyber threats, helping security teams make informed decisions. AI enables proactive threat hunting by identifying potential threats that may not be detected by automated systems, allowing cybersecurity teams to stay ahead of emerging risks. AI algorithms recognize complex patterns and trends in data, aiding in the identification of subtle and sophisticated cyber threats. Machine Learning for Adaptive Defenses. AI adapts security measures dynamically based on evolving threat landscapes, ensuring that defense mechanisms remain effective against new and emerging threats. AI systems continuously learn from new data and experiences, enhancing their ability to respond to novel and advanced cyber threats.

These AI strategies collectively contribute to a robust cybersecurity framework for protecting national infrastructure, providing a proactive and adaptive approach to defend against a wide range of cyber threats.

3. Case Studies: USA-Specific Implementations

Case studies showcasing USA-specific implementations of AI in cybersecurity highlight how advanced technologies are applied to protect critical infrastructure. Some examples that demonstrate the integration of AI in safeguarding national security include Department of Defense's Project Maven (Malmio, 2023, Downey, 2023). Project Maven objective was initiated by the Department of Defense, focuses on leveraging AI and machine learning to analyze massive amounts of data collected by drones (Suchman, 2023). AI algorithms process and analyze imagery data to identify objects, track movements, and detect anomalies, enhancing the military's situational awareness and intelligence capabilities. Another is the Cyber Threat Intelligence Sharing (Sarhan et al., 2023). Public-private partnerships facilitate threat intelligence sharing to strengthen the nation's cybersecurity posture (El-Kosairy, Abdelbaki, and Aslan, 2023). Government agencies, such as the Department of Homeland Security (DHS), collaborate with private sector entities through platforms like the Automated Indicator Sharing (AIS). AI is utilized to automate the sharing and analysis of threat indicators, enabling faster response to emerging threats (Sun et al., 2023). The third is the Financial Sector – Fraud Detection (Patel, 2023). Financial institutions employ AI to enhance fraud detection and prevent financial crimes (Reddy, 2023). Banks and financial organizations in the USA leverage machine learning algorithms to analyze transaction patterns, detect anomalies, and identify potentially fraudulent activities in real-time, thereby safeguarding financial infrastructure. Critical Infrastructure Protection - Energy Sector is another. Protecting critical infrastructure such as energy grids from cyber threats (Bosworth, and Chua, 2023). Utilities and energy companies deploy AI-based systems to monitor and analyze network traffic, detect unusual behavior, and respond to potential threats promptly (Villar Miguelez et al., 2023). AI helps in maintaining the reliability and security of energy infrastructure. Federal Bureau of Investigation (FBI) - Behavioral Analysis (Gibson, 2023). Enhancing cybersecurity investigations through advanced behavioral analysis. The FBI employs AI-driven behavioral analytics to analyze patterns of cybercriminal activity, identify threat actors, and predict potential future attacks (Sarkar, and Shukla, 2023). This approach aids in proactive threat mitigation and the apprehension of cybercriminals. National Security Agency (NSA) - Cloud Security. Securing cloud infrastructure and data against cyber threats. The NSA employs AI to monitor and analyze vast amounts of data within cloud environments. AI-driven tools enhance the detection of malicious activities, ensuring the security and integrity of sensitive information stored in the cloud. Transportation Security Administration (TSA) - Aviation Security (Kerner, 2023). Enhancing aviation cybersecurity to safeguard critical transportation systems. The TSA utilizes AI for

analyzing passenger and cargo data to identify potential security threats (Sherman, 2023). AI algorithms enhance the efficiency of security screening processes and contribute to the overall safety of the aviation sector (Satish, Mangal, and Churi, 2023). Healthcare Sector - Patient Data Security (Wenhua et al., 2023). Protecting sensitive healthcare data against cyber threats (Ali et al., 2023). Healthcare organizations employ AI to monitor and analyze network traffic, detect unusual access patterns to patient data, and prevent unauthorized access (Sharma et al., 2023). AI-driven cybersecurity measures help ensure the confidentiality and integrity of patient information.

These case studies illustrate how the USA leverages AI technologies across various sectors to bolster cybersecurity efforts, safeguard critical infrastructure, and respond effectively to emerging cyber threats.

3.1. Challenges and Ethical Considerations

The integration of AI in cybersecurity, especially for protecting national infrastructure, presents various challenges and ethical considerations that need careful attention. Some key challenges and ethical considerations associated with the use of AI in cybersecurity are here presented. AI models can be vulnerable to adversarial attacks where malicious actors manipulate inputs to deceive the system. Adversarial attacks can lead to false positives or negatives, compromising the effectiveness of AI-driven cybersecurity solutions. The need for large datasets to train AI models raises concerns about the privacy and security of sensitive information. Mishandling or unauthorized access to data can result in privacy breaches and legal repercussions. Integrating AI solutions into existing cybersecurity infrastructure can be complex, especially in heterogeneous environments. Incompatibility issues may arise, hindering the seamless integration of AI technologies with legacy systems. AI algorithms, especially deep learning models, are often viewed as black boxes, making it challenging to interpret their decision-making processes. Lack of explainability may lead to a lack of trust in AI systems, especially in critical scenarios where decision justification is essential. Training and maintaining sophisticated AI models require substantial computational resources. Resource-intensive AI solutions may pose challenges for organizations with limited budgets or less access to high-performance computing resources. The evolving nature of AI technologies makes it challenging to establish comprehensive regulatory frameworks. Inconsistent or inadequate regulations may result in ethical and legal uncertainties surrounding AI use in cybersecurity.

The key ethical considerations are here presented. AI models may inherit biases present in training data, leading to discriminatory outcomes. Biased algorithms may disproportionately affect certain demographics or groups, raising ethical concerns about fairness and justice. Ethical Use of AI in Cyber Warfare. The use of AI in offensive cyber operations raises ethical questions regarding the responsible and proportional use of technology. Lack of ethical guidelines may lead to unintended consequences, including collateral damage or escalation of cyber conflicts. Ensuring transparency in AI decision-making and holding individuals or organizations accountable for AI-driven actions is essential. Lack of accountability may undermine trust in AI systems, hindering widespread adoption and acceptance. The automation of certain cybersecurity tasks through AI may lead to job displacement for human workers. Ethical considerations involve addressing the potential socio-economic impact of AI-induced unemployment. AI technologies developed for cybersecurity can potentially be repurposed for malicious activities. Striking a balance between advancing defensive capabilities and minimizing the risk of weaponization poses ethical challenges. Users and stakeholders should be informed about the use of AI in cybersecurity and its potential implications. Lack of informed consent may lead to privacy concerns and ethical objections from individuals or communities affected by AI-driven cybersecurity measures.

Addressing these challenges and ethical considerations requires a multidisciplinary approach involving technologists, policymakers, ethicists, and the wider community to ensure responsible and beneficial use of AI in securing national infrastructure.

3.2. Collaboration and Future Directions

Collaboration and future directions in the context of AI in cybersecurity, especially for protecting national infrastructure, are critical aspects that shape the landscape of cybersecurity resilience. Establishing strong partnerships between government agencies and private industries. It lead to enhanced information sharing, joint threat intelligence efforts, and collaborative development of AI-driven cybersecurity solutions. Building and maintaining secure platforms for real-time information sharing. Timely dissemination of threat intelligence, enabling organizations to proactively defend against emerging cyber threats. Strengthening collaboration on cybersecurity at the international level. Improved global threat awareness, coordinated responses to cross-border cyber threats, and the establishment of international norms for responsible AI use in cybersecurity. Facilitating collaboration between government, private sector, and academia. Combined expertise, shared resources, and innovation for developing advanced AI solutions and addressing cybersecurity challenges. Encouraging collaboration across different critical infrastructure sectors. Holistic approaches to cybersecurity, shared best practices, and coordinated responses to threats that may impact multiple sectors simultaneously.

The future directions are here presented. Advancing research and development in Explainable AI. Enhancing transparency and interpretability of AI models to build trust and facilitate better understanding of decision-making processes in critical situations. AI for Threat Hunting and Attribution. Leveraging AI for more proactive threat hunting and attribution. Enhancing capabilities to identify and attribute cyber threats, aiding in the proactive mitigation of potential risks. Investing in the development of AI systems that are resilient to adversarial attacks. Ensuring the reliability and robustness of AI-driven cybersecurity measures in the face of evolving cyber threats. Promoting interdisciplinary research at the intersection of AI, cybersecurity, and ethics. Addressing complex challenges requires insights from diverse fields, including technology, law, ethics, and social sciences. Research and implementation of quantum-safe cryptographic algorithms. Preparing for the era of quantum computing and ensuring the long-term security of cryptographic systems. AI-Driven Policy and Regulation. Developing policies and regulations specific to AI in cybersecurity. Establishing clear guidelines for the responsible use of AI, ensuring ethical considerations are incorporated into regulatory frameworks. Cybersecurity Training and Workforce Development. Investing in education and training programs for cybersecurity professionals. Addressing the growing demand for skilled professionals who can effectively navigate the evolving landscape of AI in cybersecurity. Exploring new models of collaboration, such as federated learning and secure multi-party computation. Improving collaboration while addressing concerns related to data privacy and security in shared environments.

By prioritizing collaboration and embracing these future directions, the cybersecurity community can enhance its ability to adapt to emerging threats, develop resilient systems, and ensure the responsible use of AI in protecting national infrastructure

4. Conclusion

In conclusion, the integration of Artificial Intelligence (AI) into cybersecurity stands as a critical frontier in protecting national infrastructure, and the USA exemplifies a landscape where innovation and collaboration shape the defense against evolving cyber threats. The adoption of AI technologies brings both immense potential and a set of challenges that demand careful consideration.

The use of Machine Learning, Natural Language Processing, Neural Networks, and other AI strategies has significantly improved the speed and accuracy of threat detection, response, and overall resilience. Case studies from the USA showcase the diverse applications of AI in safeguarding critical sectors, such as defense, finance, energy, and healthcare. These implementations underline the adaptability and effectiveness of AI in addressing the dynamic nature of cyber threats.

However, challenges persist, including the risk of adversarial attacks, data privacy concerns, and the need for transparent and explainable AI models. Regulatory frameworks must evolve to keep pace with technological advancements, balancing innovation with ethical considerations to ensure responsible and accountable use of AI in cybersecurity.

The collaborative efforts between government agencies, private industries, and international partners are pivotal. Information sharing platforms, public-private partnerships, and cross-sector collaboration are fundamental for building a collective defense against cyber threats. As the cyber landscape continues to evolve, interdisciplinary research and workforce development are crucial for staying ahead of adversaries.

Looking forward, future directions involve the advancement of Explainable AI, AI-driven threat hunting, resilient AI systems, and the exploration of quantum-safe cryptography. Additionally, the development of AI-driven policies and regulations, coupled with enhanced collaboration models, will contribute to a secure and ethically sound cyber environment.

In essence, the USA's review of AI in cybersecurity for protecting national infrastructure underscores the importance of ongoing innovation, collaboration, and a commitment to ethical practices. By embracing these principles, the nation can navigate the complex cyber landscape, mitigate risks effectively, and fortify its critical infrastructure against the ever-evolving threat landscape. The journey toward a secure digital future requires continual vigilance, adaptability, and a collective commitment to the responsible integration of AI in cybersecurity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abbas, N.N., Ahmed, T., Shah, S.H.U., Omar, M. and Park, H.W., 2019. Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*, pp.1189-1211.

[2] Ali, S., Abdullah, Armand, T.P.T., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M.I. and Kim, H.C., 2023. Metaverse in healthcare integrated with explainable ai and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*, *23*(2), p.565.

[3] Bharadiya, J.P., 2023. AI-Driven Security: How Machine Learning Will Shape the Future of Cybersecurity and Web 3.0. *American Journal of Neural Networks and Applications*, *9*(1), pp.1-7.

[4] Bobish, M., 2023. Sharing Cyber Threat Information Between the United States' Public and Private Sectors (Doctoral dissertation, Utica University).

[5] Bosworth, K. and Chua, C., 2023. The countersovereignty of critical infrastructure security: Settler-state anxiety versus the pipeline blockade. *Antipode*, *55*(5), pp.1345-1367.

[6] Chakraborty, A., Biswas, A. and Khan, A.K., 2023. Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3-25). Cham: Springer International Publishing.

[7] de Azambuja, A.J.G., Plesker, C., Schützer, K., Anderl, R., Schleich, B. and Almeida, V.R., 2023. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), p.1920.

[8] Djenna, A., Barka, E., Benchikh, A. and Khadir, K., 2023. Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. *Sensors*, *23*(14), p.6302.

[9] Downey, A., 2023. Algorithmic predictions and pre-emptive violence: artificial intelligence and the future of unmanned aerial systems. *Digital War*, pp.1-11.

[10] El-Kosairy, A., Abdelbaki, N. and Aslan, H., 2023. A survey on cyber threat intelligence sharing based on Blockchain. *Advances in Computational Intelligence*, *3*(3), p.10.

[11] Gibson, K., 2023. Pathway to Targeted Violence: Can Early Intervention Work?. *Dep't of Just. J. Fed. L. & Prac.*, *71*, p.39.

[12] Halim, Z., Sulaiman, M., Waqas, M. and Aydın, D., 2023. Deep neural network-based identification of driving risk utilizing driver dependent vehicle driving features: A scheme for critical infrastructure protection. *Journal of Ambient Intelligence and Humanized Computing*, *14*(9), pp.11747-11765.

[13] Heilig, T. and Scheer, I., 2023. Decision Intelligence: Transform Your Team and Organization with AI-Driven Decision-Making. John Wiley & Sons.

[14] Islam, M.A., 2023. Application of artificial intelligence and machine learning in security operations center. *Issues in Information Systems*, *24*(4).

[15] Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, p.101804.

[16] Kayode-Ajala, O., 2023. Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), pp.1-21.

[17] Kerner, F., 2023. An Interview with Francine Kerner: Chief Counsel of the Transportation Security Administration. *Air and Space Lawyer*, *35*(3), pp.4-7.

[18] Khang, A., Gupta, S.K., Rani, S. and Karras, D.A. eds., 2023. Smart Cities: IoT Technologies, Big Data Solutions, Cloud Platforms, and Cybersecurity Techniques. CRC Press. `

[19] Khonturaev, S.I., Khoitkulov, A.A. and Abdullayeva, M.R., 2023. Revolutionizing Security: The Transformative Role Of Artificial Intelligence. *Лучшие интеллектуальные исследования*, *7*(2), pp.129-135.

[20] Kumar, S., Gupta, U., Singh, A.K. and Singh, A.K., 2023. Artificial Intelligence: Revolutionizing cyber security in the Digital Era. *Journal of Computers, Mechanical and Management*, *2*(3), pp.31-42.

[21] Lemieux, F., 2023. Digital Transformation and Artificial Intelligence: Opportunities and Challenges. *Digital Strategies And Organizational Transformation*, pp.103-117.

[22] Majid, A.A.M., Alshaibi, A.J., Kostyuchenko, E. and Shelupanov, A., 2023. A review of artificial intelligence based malware detection using deep learning. *Materials Today: Proceedings*, *80*, pp.2678-2683.

[23] Malmio, I., 2023. Ethics as an enabler and a constraint–Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. *Technology in Society*, *72*, p.102193.

[24] Mishra, S., 2023. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences*, *13*(10), p.5875.

[25] Moorthy, R.S.S. and Nathiya, N., 2023. Botnet detection using artificial intelligence. *Procedia Computer Science*, *218*, pp.1405-1413.

[26] Patel, K., 2023. Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques. *International Journal of Computer Trends and Technology*, *71*(10), pp.69-79.

[27] Pinto, A., Herrera, L.C., Donoso, Y. and Gutierrez, J.A., 2023. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors*, *23*(5), p.2415.

[28] Rawindaran, N., 2023. *Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales* (Doctoral dissertation, Cardiff Metropolitan University).

[29] Reddy, S.R.B., 2023. Large Scale Data Influences Based on Financial Landscape Using Big Data. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(4), pp.3862-3870.

[30] Rich, M.S., 2023. Cyberpsychology: A Longitudinal Analysis of Cyber Adversarial Tactics and Techniques. *Analytics*, *2*(3), pp.618-655.

[31] Roba Abbas, K.M., Pitt, J., Vogel, K.M. and Zafeirakopoulos, M., Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap.

[32] Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), p.13369.

[33] Sanni, O., Adeleke, O., Ukoba, K., Ren, J. and Jen, T.C., 2024. Prediction of inhibition performance of agro-waste extract in simulated acidizing media via machine learning. *Fuel*, *356*, p.129527.

[34] Sarhan, M., Layeghy, S., Moustafa, N. and Portmann, M., 2023. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, *31*(1), p.3.

[35] Sarker, I.H., 2023. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, *10*(6), pp.1473-1498.

[36] Sarkar, G. and Shukla, S.K., 2023. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, p.100034.

[37] Satish, A.S., Mangal, A. and Churi, P., 2023. A systematic review of passenger profiling in airport security system: Taking a potential case study of CAPPS II. *Journal of transportation security*, *16*(1), p.8.

[38] Sherman, T.W., 2023. Aviation Security: TSA Could Better Ensure Detection and Assess the Potential for Discrimination in Its Screening Technologies (No. GAO-24-107094).

[39] Sharma, P., Namasudra, S., Crespo, R.G., Parra-Fuente, J. and Trivedi, M.C., 2023. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, *629*, pp.703-718.

[40] Solar, C., 2023. Cybersecurity Governance in Latin America: States, Threats, and Alliances. State University of New York Press.

[41] Srinivasan, R., Kavitha, M., Kavitha, R. and Uma, S., 2023, June. Cybersecurity and Artificial Intelligence: A Systematic Literature Review. In *Recent Trends in Computational Intelligence and Its Application: Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22)* (p. 339). CRC Press.

[42] Štitilis, D., Laurinaitis, M. and Verenius, E., 2023. The Use of biometric technologies in ensuring critical infrastructure security: the context of protecting personal data. *Entrepreneurship and sustainability issues*, *10*, pp.133-150.

[43] Suchman, L., 2023. Imaginaries of omniscience: Automating intelligence in the US Department of Defense. *Social Studies of Science*, *53*(5), pp.761-786.

[44] Sufi, F., 2023. A New AI-Based Semantic Cyber Intelligence Agent. *Future Internet*, *15*(7), p.231.

[45] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y. and Zhang, J., 2023. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*.

[46] Turgay, M., 2023. The impact of artificial intelligence on cybersecurity. *Вестник Науки и Творчества*, (3 (85)), pp.51-53.

[47] Tuteja, V. and Marwaha, S.S., 2023. Artificial intelligence: threat of terrorism and need for better counter-terrorism efforts. *International Journal of Creative Computing*, *2*(1), pp.87-100.

[48] Uzoma, J., Falana, O., Obunadike, C., Oloyede, K. and Obunadike, E., 2023. Using artificial intelligence for automated incidence response in cybersecurity. *International Journal of Information Technology (IJIT)*, *1*(4).

[49] Villar Miguelez, C., Monzon Baeza, V., Parada, R. and Monzo, C., 2023. Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities*, *6*(2), pp.728-743.

[50] Wenhua, Z., Qamar, F., Abdali, T.A.N., Hassan, R., Jafri, S.T.A. and Nguyen, Q.N., 2023. Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), p.546.

[51] Xia, L., Semirumi, D.T. and Rezaei, R., 2023. A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*, p.104771