Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Systematic Literature Review on Enhancing National Security Strategy Using Artificial Intelligence Threat and Challenges for Sustainable Security

Ali Saeed Khalfan Bin Marran Aldhaheri, Mohd Mizan Mohammad Aslam & Wong Choi Ye
Strategic & Defence Studies
National Defence University of Malaysia, 57000 Kuala Lumpur

ARTICLE INFO

Received: 20 June 2024

Accepted: 06 Aug 2024

ABSTRACT

When it comes to matters of national security, artificial intelligence (AI) has completely taken over the conventional security frameworks. The efficiency of decision-making, threat identification, and surveillance has all been significantly improved as a result of this. The deployment of this product comes with a number of challenging issues, some of which include cyber vulnerabilities, ethical conundrums, and the risk of aggressive exploitation. Within the framework of national security, this study conducts a complete literature review in order to gain a better understanding of the potential, hazards, and approaches for long-term deployment of artificial intelligence. By conducting a comprehensive assessment of relevant literature, policy papers, and case studies, this study draws attention to significant advancements in artificial intelligence-driven security technologies. These advancements include deep learning models, autonomous surveillance, and predictive analytics. Regulatory flaws, cybersecurity concerns, misinformation, and algorithmic discrimination are many of the significant issues that are included in this report. The project continues on to evaluate risk mitigation strategies, such as ethical AI governance, adversarial AI resistance, and international regulatory frameworks, with the intention of ensuring the deployment of artificial intelligence in a safe and responsible manner. By synthesizing the information that is already available, this analysis helps to fill in the gaps in our understanding of how to incorporate artificial intelligence into national security policies while simultaneously reducing the risks. The findings shed light on the significance of a comprehensive strategy that capitalizes on the features that AI possesses while simultaneously minimizing the vulnerabilities that it possesses in terms of security. This work contributes to the continuing discussion on national security policy that is powered by artificial intelligence by shining light on possible routes for future research and shedding light on sustainable security practices.

Keywords: Artificial Intelligence, National Security Strategy, Systematic Literature Review

1. Introduction

The integration of artificial intelligence into national security has resulted in a significant shift in the manner in which nations address the newly emerging threats to national security. The field of defense is undergoing a profound transformation as a result of the introduction of artificial intelligence technologies such as autonomous surveillance and predictive threat analytics. The integration, on the other hand, does not come without any risks. The purpose of this study is to conduct an in-depth investigation into the twin-edged sword that is artificial intelligence (AI), namely its strategic worth and the potential threat it poses to the nation's security in the long term. The purpose of this research is to give a comprehensive literature review on the subject of the incorporation of artificial intelligence into national security policies. The use of artificial intelligence (AI) has the potential to enhance capabilities in areas such as threat identification, decision-making, and monitoring; but, it also presents significant challenges, such as ethical dilemmas, algorithmic biases, and cyber threats. The objective of this research is to consolidate the existing body of literature on artificial intelligence (AI) in security contexts and to identify significant themes, hazards, and strategies for mitigating such risks. The purpose of this study is to provide a strategic roadmap for the responsible and sustainable deployment of artificial intelligence in national security. The roadmap is based on case studies and governance frameworks from around the world. The findings contribute to the development of a comprehensive, ethical, and technologically advanced plan for national security for the country.

2.0 Literature Review

The plan for national security often develops in unison with the most pressing issues and recent successes of society. Both of these aspects are replete with modern threats and opportunities, as well as the resources that are available to us to combat them. It is possible for a strategy that follows global trends and adopts an appropriate analytical approach to reflect a well-defined national objective, a path to accomplishing that purpose, and the state's capacity to deploy instruments of national power to achieve that interest. All of these elements can be expressed in a strategy. All of the different forms that artificial intelligence can take will have a significant influence on the development of society in the course of the future. To a significant extent, the implementation style will be determined by the requirements and capabilities of the state. The ultimate goal of the study is to increase knowledge of artificial intelligence among professionals and, by extension, to make it a central topic for future conversations regarding national defense and security. As the spread of technology continues to permeate every aspect of society, it will undoubtedly find its way into doctrinal and strategic texts that are relevant to defense. According to the findings of this expert's research, incorporating and operationalizing artificial intelligence must be one of the initial steps in the process of building a modern national security policy.

It has been demonstrated that artificial intelligence (AI) has enhanced capabilities in decision-making, threat identification, and surveillance. Furthermore, the incorporation of AI into national security has resulted in a transformation of traditional security procedures. On the other hand, artificial intelligence is associated with a number of significant challenges, including the potential for cyber threats, ethical concerns, and the chance that it could be abused by malevolent individuals. The purpose of this article is to study potential strategic applications of artificial intelligence to boost national security. This is done in light of the dangers and obstacles that come with deploying AI. The purpose of this research is to investigate the role that artificial intelligence plays in the existing security frameworks. The goal of this research is to develop a sustainable security plan that strikes a balance between technological innovation and risk reduction. Since the beginning of time, the most important aspects of national security have been the collection of intelligence, the implementation of military defenses, and the implementation of cybersecurity measures. The emergence of artificial intelligence has transformed a variety of fields in a number of different ways, including the ability to make autonomous decisions, perform predictive analytics, and analyze data quickly. Security applications that are powered by artificial intelligence, such as facial recognition, autonomous drones, and cybersecurity defenses, are receiving a significant amount of funding from governments all over the world in order to confront threats that are always evolving. The rapid application of artificial intelligence in topics pertaining to national security, on the other hand, has been the subject of grave concerns. Threats to security that are of significant importance include cyberattacks that are powered by artificial intelligence, deepfake disinformation operations, and algorithmic biases. Additionally, in order to guarantee the responsible deployment of AI-driven security solutions, comprehensive regulatory frameworks are required. This is because of the ethical and legal ramifications that these solutions may have. This study's objective is to investigate the potential advantages, disadvantages, and adverse effects that could arise from incorporating AI into national security strategies.

2.1 Artificial Intelligence (AI) in National Security

Artificial intelligence (AI) has emerged as an essential component of modern national security strategy due to its ability to enhance intelligence gathering, cybersecurity, and military applications. Among the many studies that have investigated the ways in which artificial intelligence (AI) may change national security systems, Allen and Goldston (2024) and Schmidt and Work (2021) are only two examples. Buchanan (2024) says that artificial intelligence-driven threat detection and risk assessment models have significantly improved the response times of cybersecurity operations due to their use. According to Blasch et al. (2019), autonomous surveillance technology such as facial recognition and drone reconnaissance have also had a significant impact on intelligence operations throughout this time period. In addition, according to the Department of Homeland Security, by the year 2024, national security organizations will be able to process enormous amounts of intelligence data in real time thanks to analytics that are driven by artificial intelligence. As a result, this will make it possible to conduct predictive threat assessments and to react quickly to emerging security concerns. (Taddeo et al., 2019) It has been demonstrated that artificial intelligence-enhanced intelligence analysis has revolutionized military strategies by enabling the detection and elimination of potential threats to national security in advance. However, despite these advancements, concerns over the regulation of artificial intelligence continue to be of vital importance. The National Security Commission on Artificial Intelligence (NSCAI) (2021) asserts that it is impossible to permit an ethical use of artificial intelligence in defense and surveillance without regulatory oversight. Matania and Rapaport (2021) claim that there are legal and ethical problems regarding the possibility for algorithmic discrimination and bulk data collection that come along with artificial intelligence (AI), despite the fact that AI does increase operational efficiency.

2.2 Potential Threats Posed by AI

Despite the fact that artificial intelligence has many advantages, it also poses a variety of dangers to the nation's security. A number of issues, including cybercrime, hostile AI attacks, and deepfake-driven misinformation campaigns, have lately come to light (Floridi & Taddeo, 2018; Musser et al., 2023). According to Georgetown University's research from 2023, cyberattacks that are powered by artificial intelligence have the potential to compromise crucial infrastructure by manipulating security systems. Li (2024) sheds light on the potential for the weaponization of deepfake technology and artificial intelligence-generated disinformation to erode public faith in digital information and political stability. This potential is brought to light by the statement. According to Mikhailov (2023), security organizations are going to be confronted with a substantial threat from hostile artificial intelligence. This threat arises when machine learning models are modified in order to generate false positives or to evade detection. Project MUSE (2025) suggests that thieves may be able to overcome cybersecurity measures and undermine frameworks for national security by exploiting gaps in AI-driven security systems. This is according to the findings of the project. In addition, autonomous weapons that are powered by artificial intelligence provide vulnerabilities that, if not adequately supervised, could lead conflicts to grow in an uncontrollable manner (Musser et al., 2023). There has been an increase in the employment of artificial intelligence-driven disinformation operations by both state and non-state actors in order to exert influence over public opinion and undermine democratic procedures. In accordance with the assertions made by Li (2024), the utilization of deepfake videos that are produced by artificial intelligence has the potential to affect the outcomes of elections and to aggravate hostilities abroad. According to the Department of Homeland Security (2024), the dissemination of misleading information that is produced by artificial intelligence has the potential to weaken international security systems to the extent that effective actions are not made.

2.3 Ethical and Legal Concerns in AI Deployment

The possibility of widespread application of artificial intelligence for military purposes raises significant ethical and legal concerns. According to Taddeo et al. (2019), the installation of AI-driven surveillance systems has the potential to violate civil liberties in authoritarian regimes. This is because such technologies could be used to suppress dissent in such regimes. There is also a significant amount of evidence that artificial intelligence models reflect the biases that are present in the data that is used to train them, which has resulted in worries around algorithmic bias (Buchanan, 2024). The European Union has reportedly proposed stringent regulations in order to combat bias in artificial intelligence and to guarantee parity in security applications that are powered by AI, as stated by Sommer et al. (2023). In spite of this, Floridi and Taddeo (2018) state that ethical governance of artificial intelligence should incorporate human monitoring, accountability, and transparency in addition to legislative processes. This is done with the goal of cutting down on any potential negative consequences. The National Security Commission on Artificial Intelligence (2021) emphasizes the significance of global collaboration in the development of global ethical frameworks for artificial intelligence in order to prevent the possibility of the technology being abused for the goal of national security.

In an effort to mitigate the effects of hazards associated with artificial intelligence, researchers have proposed a variety of policy and governance approaches. Algorithmic transparency and explainable artificial intelligence (XAI) models, as stated by Taddeo, McCutcheon, and Floridi (2019), can be of assistance in generating confidence in security applications that are powered by artificial intelligence. XAI approaches are designed to make decisions that can be understood and justified by artificial intelligence in order to reduce the possibility of algorithmic errors and biases. According to the findings of a comparative study conducted by Sommer, Matania, and Hassid (2023), countries that have more severe laws for artificial intelligence, such as the European Union, have less security risks regarding AI than countries that have less regulation. Legislative frameworks such as the European Union's Artificial Intelligence Act are being established in order to establish legal requirements for the ethical deployment of artificial intelligence in sensitive security scenarios (Floridi & Taddeo, 2018). In addition, Project MUSE (2025) emphasizes the importance of implementing cybersecurity policies for artificial intelligence, such as adversarial training methodologies, in order to reduce the likelihood of cyberattacks on AI. When it comes to preventing threats to the security of artificial intelligence, international cooperation is absolutely necessary. According to The Guardian (2025), the Paris AI Safety Declaration is one of several international initiatives that are attempting to establish principles for the governance of artificial intelligence that are relevant across national boundaries. According to Reveron and Savage (2024), improved cybersecurity collaboration between the governments of the United States and the European Union has boosted collective AI resilience, thereby minimizing the effects of cyberattacks driven by artificial intelligence.

Artificial intelligence security frameworks should include systems to detect anomalies in AI behavior, real-time threat intelligence, and adversarial defense mechanisms, according to the Department of Homeland Security (2024). This is in order to combat cyberattacks that are driven by artificial intelligence. Based on the findings of the research, it is possible for governments and technology companies to collaborate in public-private partnerships in order to set privacy and safety norms for artificial intelligence. AI has the potential to be both beneficial and detrimental to the nation's security, as indicated by the research that was examined. While artificial intelligence (AI) is improving cybersecurity, threat detection, and surveillance, it also introduces a number of hazards, such as adversarial AI, disinformation, and cyber vulnerabilities. According to the findings of prior research, it is essential to have robust legal frameworks, worldwide collaboration, and the ethical deployment of artificial intelligence in order to address these concerns. Legislators should address issues of bias in artificial intelligence, concerns about privacy, and algorithmic openness in order to better guarantee the ethical use of AI in security applications. The findings of this literature analysis will serve as the foundation for the subsequent chapters of the study, which will focus on real-world case studies, policy ideas, and strategies for enhancing national security through the application of artificial intelligence. The following chapter will provide a comprehensive discussion of research methodologies, which will include the procedures for collecting data, interpreting it, and considering any ethical concerns that may be pertinent.

2.4 Strategies for AI Risk Mitigation

In an effort to mitigate the effects of hazards associated with artificial intelligence, researchers have proposed a variety of policy and governance approaches. According to Taddeo, McCutcheon, and Floridi (2019), it is possible to meet the goal of building confidence in AI-driven security applications by utilizing explainable AI models and algorithmic transparency. When explainable artificial intelligence approaches are utilized, the risk of algorithmic errors and unintended biases is reduced. This is because the judgments made by AI are able to be interpreted and defended. According to the findings of a comparative study conducted by Sommer, Matania, and Hassid (2023), countries that have more severe laws for artificial intelligence, such as the European Union, have less security risks regarding AI than countries that have less regulation. Legislative frameworks such as the European Union's Artificial Intelligence Act are being established in order to establish legal requirements for the ethical deployment of artificial intelligence in sensitive security scenarios (Floridi & Taddeo, 2018). In addition, Project MUSE (2025) emphasizes the importance of implementing cybersecurity policies for artificial intelligence, such as adversarial training methodologies, in order to reduce the likelihood of cyberattacks on AI.

When it comes to preventing threats to the security of artificial intelligence, international cooperation is absolutely necessary. According to The Guardian (2025), the Paris AI Safety Declaration is one of several international initiatives that are attempting to establish principles for the governance of artificial intelligence that are relevant across national boundaries. According to Reveron and Savage (2024), improved cybersecurity collaboration between the governments of the United States and the European Union has boosted collective AI resilience, thereby minimizing the effects of cyberattacks driven by artificial intelligence. Artificial intelligence security frameworks should include systems to detect anomalies in AI behavior, real-time threat intelligence, and adversarial defense mechanisms, according to the Department of Homeland Security (2024). This is in order to combat cyberattacks that are driven by artificial intelligence. Based on the findings of the research, it is possible for governments and technology companies to collaborate in public-private partnerships in order to set privacy and safety norms for artificial intelligence.

AI has the potential to be both beneficial and detrimental to the nation's security, as indicated by the research that was examined. While artificial intelligence (AI) is improving cybersecurity, threat detection, and surveillance, it also introduces a number of hazards, such as adversarial AI, disinformation, and cyber vulnerabilities. Studies that have been done in the past have emphasized the importance of robust regulatory frameworks, global collaboration, and the ethical deployment of artificial intelligence in order to mitigate the impact of these risks. Legislators should address issues of bias in artificial intelligence, concerns about privacy, and algorithmic openness in order to better guarantee the ethical use of AI in security applications.

The findings of this literature analysis will serve as the foundation for the subsequent chapters of the study, which will focus on real-world case studies, policy ideas, and strategies for enhancing national security through the application of artificial intelligence. The following chapter will provide a comprehensive discussion of research methodologies, which will include the procedures for collecting data, interpreting it, and considering any ethical concerns that may be pertinent.

3.0 Objective

The primary objective of this study is to carry out an in-depth investigation into the incorporation of artificial intelligence into national security plans. The objective is to conduct a systematic literature review (SLR) with the purpose of determining the transformative benefits, rising risks, and strategic obstacles that are related with the deployment of artificial intelligence. It is becoming increasingly clear that artificial intelligence (AI) is a double-edged sword as an increasing number of countries use AI capabilities such as autonomous surveillance systems, decision-making algorithms, and predictive analytics into their defense and security policies. With the goal of maximizing the potential of artificial intelligence (AI) while minimizing its potential risks, the purpose of this research is to investigate the existing literature on the subject of artificial intelligence (AI) and its potential advantages and disadvantages in relation to the infrastructure of national security. The lack of robust international frameworks for the governance of artificial intelligence, algorithmic bias in security operations, deepfake-based misinformation campaigns, and adversarial AI attacks are all instances of such problems.

This study's overarching objective is to establish a methodical and strategic framework that can apply artificial intelligence for national security in a way that is both sustainable and responsible. This will be accomplished by studying these complicated concerns. All of these things are included in this: methods for international cooperation, public-private partnerships, ethical governance principles for artificial intelligence, and regulatory measures. Within the context of the artificial intelligence-security nexus, the study intends to identify current knowledge gaps in addition to making specific recommendations for measures to be taken by policymakers, defense institutions, and technology developers. This will ensure that artificial intelligence can improve security without putting civil rights, international peace and harmony, or moral principles in jeopardy. In conclusion, the research contributes to the larger conversation about security in the digital age by providing a multi-faceted view that combines the principles of openness, responsibility, and resilience with the advancement of technology.

4.0 Methodology

This section provides an explanation of the approach that was utilized in the research project, which was a systematic literature review (SLR). We decided to use the SLR technique in order to conduct an in-depth, open, and reproducible analysis of the academic work that has been done on the intersection of artificial intelligence and national security.

The systematic literature review (SLR) method allows researchers to systematically collect, evaluate, and synthesize relevant academic literature, therefore identifying themes, gaps, and implications.

4.1 Rationale for Using Systematic Literature Review

In light of the growing complexity and multidisciplinary nature of the application of artificial intelligence in national security, it is necessary to take a methodical approach to the synthesis of the most recent research. There are a number of possible problems that can arise with traditional narrative literary evaluations, including subjectivity, incompleteness, and an inability to duplicate results. On the other hand, a systematic literature review adheres to a protocol-driven procedure, which helps to bring about a reduction in bias while simultaneously increasing the validity and dependability of the findings. The selection of the SLR methodology was based on its capacity to generate high-quality evidence to influence academic and policy discourse, as well as its methodical approach to managing big datasets. Both of these factors contributed to the decision.

4.2 Review Protocol Design

For the purpose of conducting the systematic review, a detailed protocol was designed in accordance with the requirements established by PRISMA, which stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses. Methods for data extraction, strategies for synthesis, criteria for quality assessment, databases that were accessed, search strings, and research questions were all outlined in the protocol. As the foundation for the study, the following significant research concerns were taken into consideration:

RQ1: Taking into account ethical concerns while incorporating artificial intelligence into national security projects is the first question that needs to be answered.

RQ2: What are the most serious threats that artificial intelligence (AI) generates in the context of applications that pertain to national security?

RQ3: what measures may be implemented by governments and security organizations to lessen the possible risks associated with security measures that are supported by artificial intelligence?

These questions served as a source of inspiration for both the inclusion criteria and the approach for developing the theme analysis. The comprehensive search strategy included the utilization of scholarly databases such as Scopus, Web of Science, IEEE Xplore, SpringerLink, and Google Scholar, amongst others. The outcomes under each subject were reported using a technique called narrative synthesis. This was supported with direct quotations and comparative analysis across different policy contexts and locales.

4.3 Validation and Reliability Measures

The Cohen's Kappa statistic was utilized in order to ascertain the inter-rater reliability for the initial screening. This was done with the intention of the review being more reliable. At regular intervals, calibration procedures were carried out in order to guarantee that the coding was constant. Sharing coded theme summaries with subject matter experts in the industry so that they may verify them was yet another way that was utilized for the purpose of member checking. Due to the fact that the research was limited to papers written in English, it is possible that there is relevant work that was written in other languages but was not included in the study. Because of restrictions on access, gray literature and classified government documents were not included in the collection. The evaluation does not include any longitudinal source data because its primary focus is on synthesising secondary studies. The SLR technique did an excellent job of organizing and summarizing the current state of the art in artificial intelligence and national security research, despite the inclusion of these caveats.

4.4 Ethical Considerations

Due to the fact that this work adhered to ethical research requirements, all sources were appropriately credited, and the rights to intellectual property were honored. Before conducting any interviews or communications, we made sure to follow the standards of the institution's ethics and gain informed consent from the experts. This allowed us to verify the expertise of the individuals involved. In order to go deeper into the topics that were being investigated, a procedure known as a systematic literature review was utilized to collect data that was of high quality and relevant. The open approach, which promotes the legitimacy and reproducibility of the results, lays a solid foundation for policy ideas and subsequent academic inquiry. This is a significant advantage.

4.5 Result & Discussion

In spite of the growing amount of research on artificial intelligence in national security, there is still a lack of a comprehensive and standardized framework that includes AI risk assessment, governance policies, ethical concerns, adversary resilience, and performance evaluation into a single security strategy. Research in this area has, up until this point, paid no attention to the requirement of a comprehensive national security framework. Instead, it has concentrated on specific areas, such as cybersecurity applications (Blasch et al., 2019; Buchanan, 2024), adversarial artificial intelligence threats (Mikhailov, 2023; Project MUSE, 2025), and ethical considerations (Taddeo et al., 2019; Georgetown University, 2023). Despite the fact that regulatory efforts such as the EU AI Act (Sommer et al., 2023) and NSCAI recommendations (NSCAI, 2021) provide guidance on ethical AI deployment, there is a lack of specific enforcement mechanisms and cross-border governance measures to mitigate the exploitation of artificial intelligence in security operations.

Additionally, there is a lack of standardized performance metrics to evaluate the effectiveness of artificial intelligence in security operations, and the research that is currently being conducted does not delve far enough into practical defenses against hostile AI attacks (Buchanan, 2024; Li, 2024 respectively). A further issue that contributes to this gap is the absence of empirical research that particularly investigates the ways in which artificial intelligence (AI) influences security policy and the stability of geopolitical systems (Reveron & Savage, 2024; The Guardian, 2025).

This study will propose an all-encompassing artificial intelligence security paradigm that applies to the following areas in order to close this gap:

i. A complete model for evaluating the dangers that are linked with artificial intelligence (AI), which includes cybersecurity, AI that is hostile to humans, and disinformation.

ii. A system of laws and regulations to control AI security, including mechanisms for international cooperation and regulation.

iii. These guidelines for ethical behavior and ways to decrease prejudice in artificial intelligence were established expressly for use in applications related to national security.

iv. Precautions to be taken in order to safeguard artificial intelligence systems from attacks by hostile AI.

v. In order to measure how well artificial intelligence performs in national security activities, performance metrics are required.

This research will address these multiple challenges using a unified strategy, which will contribute to the construction of a national security policy that is intelligently led by artificial intelligence that is sustainable, robust, and morally oriented.

5.0 Conclusion

The purpose of this study was to provide a summary of the studies that have investigated the application of artificial intelligence (AI) in national security, highlighting both the positive and negative aspects of this technology. In the beginning of the chapter, some background information on the study was presented, with the primary focus being on the ways in which AI-driven technologies are affecting national security. The statement of the problem brought to light significant security problems, including cyberattacks, ethical conundrums, and vulnerabilities in the regulatory framework. This research was conducted with the intention of analyzing the application of artificial intelligence (AI) in security strategy, determining the potential dangers that could arise, and presenting viable methods to mitigate or eradicate those dangers. The significance of the study was emphasized, with particular attention paid to the applicability of the study to academics, government agencies, and political figures. Cybersecurity, surveillance, and strategic defense were the key areas of attention for the study, which acknowledged constraints such as a lack of access to classified military artificial intelligence programs in its scope and restrictions but emphasized the importance of these areas. As part of the methodological approach that was presented in the study, the following components were included: literature reviews, case studies, expert interviews, thematic analysis, comparative analysis, and policy evaluation. These methodologies allow for a comprehensive investigation into the effects that artificial intelligence has on national security. After this chapter lays the framework with a comprehensive literature review, the subsequent chapters will provide a comprehensive methodology, findings, comments, and conclusions. Following that, we will be delving into a complete literature review that will cover all the bases, including recent studies on the applications of artificial intelligence, security issues, regulatory frameworks, and national security ethics.

References:

[1] Allen, G. C., & Goldston, I. (2024, October 25). The Biden administration's National Security Memorandum on AI explained. Center for Strategic and International Studies. https://www.csis.org/analysis/biden-administrations-national-security-memorandum-ai-explained.

[2] Blasch, E., Sung, J., Nguyen, T., Daniel, C. P., & Mason, A. P. (2019). Artificial intelligence strategies for national security and safety standards. arXiv preprint arXiv:1911.05727. https://arxiv.org/abs/1911.05727.

[3] Buchanan, B. (2024). A national security research agenda for cybersecurity and artificial intelligence. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/a-national-security-research-agenda-for-cybersecurity-and-artificial-intelligence.

[4] Department of Homeland Security. (2024, November 14). Groundbreaking framework for the safe and secure deployment of AI in critical infrastructure. https://www.dhs.gov/archive/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure.

[5] Floridi, L., & Taddeo, M. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6.

[6] Georgetown University. (2023). Adversarial machine learning and cybersecurity: Risks, challenges, and legal implications. arXiv preprint arXiv:2305.14553. https://arxiv.org/abs/2305.14553.

[7] King, L. (2024, December 1). Commentary: The backdoor challenge of AI machine-learning. Journal-Courier. https://www.myjournalcourier.com/opinion/article/the-backdoor-challenge-ai-learning-19980851.php.

[8] Li, B. (2024, August 15). Researchers have ranked AI models based on risk—and found a wild range. WIRED. https://www.wired.com/story/ai-models-risk-rank-studies.

[9] Matania, E., & Rapaport, A. (2021). CYBERMANIA: How Israel became a global powerhouse in the domain that is revolutionizing the future of humanity. Cybertech-Arrowmedia..

[10] Matania, E., & Sommer, U. (2023). Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations. International Relations. https://doi.org/10.1177/00471178231211500

[11] Mikhailov, D. I. (2023). Optimizing national security strategies through LLM-driven artificial intelligence integration. arXiv preprint arXiv:2305.13927. https://arxiv.org/abs/2305.13927.

[12] Musser, M., Lohn, A., Dempsey, J. X., Spring, J., Siva Kumar, R. S., Leong, B., Liaghati, C., Martinez, C., Grant, C. D., Rohrer, D., Frase, H., Elliott, J., Bansemer, J., Rodriguez, M., Regan, M., Chowdhury, R., & Hermanek, S. (2023). Adversarial machine learning and cybersecurity: Risks, challenges, and legal implications. arXiv preprint arXiv:2305.14553. https://arxiv.org/abs/2305.14553.

[13] National Security Commission on Artificial Intelligence. (2021). Final report. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[14] Project MUSE. (2025). National security concerns for artificial intelligence. Project MUSE. https://muse.jhu.edu/article/950955.

[15] Reveron, D., & Savage, J. (2024, December 1). Commentary: The backdoor challenge of AI machine-learning. Journal-Courier. https://www.myjournalcourier.com/opinion/article/the-backdoor-challenge-ai-learning-19980851.php.

[16] Schmidt, E., & Work, R. (2021). Final report. National Security Commission on Artificial Intelligence. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[17] Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. Political Science, 75(2), 140–164. https://doi.org/10.1080/00323187.2023.2278499.

[18] Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6.

[19] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1.

[20] The Australian. (2025, February 4). DeepSeek threat: 'Act now or be obliterated'. The Australian. https://www.theaustralian.com.au/business/technology/deepseek-threat-act-now-or-be-obliterated-tech-council-warns/news-story/24306d28f303052126ee20dc4c6d17e3.

[21] The Guardian. (2025, February 11). US and UK refuse to sign Paris summit declaration on 'inclusive' AI. The Guardian. https://www.theguardian.com/technology/