

Exploring the nexus of artificial intelligence, fake news and defense strategy

Wildan Akbar Hashemi Rafsanjani ^{1*}, Herlina Juni Risma Sarah ¹, Guntur Eko Saputro ¹,
Luhut Simbolon ¹

¹⁾ The Republic of Indonesia Defense University, Jawa Barat

Received December 05, 2024/Accepted September 29, 2025

Abstract

The advancement of artificial intelligence (AI) has significantly impacted digital communication, including the creation and dissemination of disinformation. Technologies such as deepfakes, chatbots powered by natural language processing (NLP), and generative algorithms enable the production of false information that is challenging to distinguish from reality, posing a threat to information security and global stability. In the defense context, AI-driven disinformation can be weaponized in information warfare, undermining public trust, creating social disorientation, and weakening national security strategies. This study examines how AI is utilized to spread disinformation and its implications for defense strategies. Through case studies and literature analysis, the research highlights the urgent need for robust mitigation measures, including the development of AI-based detection technologies, the enhancement of digital literacy, and global collaboration in regulating the use of AI. The findings offer insights into the strategic threats posed by AI to defense systems, while providing recommendations to strengthen resilience against AI-driven disinformation attacks.

Keywords: artificial intelligence; fake new; information security; information warfare

Introduction

The development of artificial intelligence (AI) technology has had a profound impact on various aspects of human life. One significant implication of this advancement is how AI is used to create and disseminate disinformation, which now poses a real threat to global security, social stability, and national defense systems. AI-driven disinformation has reached new levels of scale and effectiveness through technologies such as deepfakes, chatbots powered by natural language processing (NLP), and generative algorithms, which enable the manipulation of information that is difficult to distinguish from facts (Shoaib et al., 2023).

According to Benzie & Montasari (2022), there is undoubtedly a complex relationship between lies spread through AI methods such as bots and the humans involved in the content and spreading it within their networks. Thus, misinformation and disinformation are intertwined online, which can worryingly be further spread by humans in the real world. Therefore, it is clear that the problems caused by the spread of misinformation and disinformation are multifaceted and adapt rapidly with technological advances.

Nazar & Bustam (2020) stated that the fatality rate caused by AI has increased with the emergence of Deepfake technology. Deepfake has become a real problem that requires public attention due to its misuse. Deepfake itself is very useful in filmmaking, but it is precisely because of the cases of misuse that have given it a bad reputation in the media. Deepfake's face-swapping feature can indeed produce realistic-looking videos, but the world is not yet ready for it. Most people are still unaware of Deepfake, so they may mistake Deepfake videos for real videos that have not been altered or computer-generated. The ability to easily and cheaply generate convincing images, audio, and video through artificial intelligence will impact politics, privacy, law, security, and, more broadly, society. Elhoussainy (2024) revealed that political news, particularly government-related news, is the most frequently faked, especially during times of political turmoil. This fake news is often spread to support government goals, gain public sympathy, and serve the interests of specific political parties

*Corresponding Author:

E-mail: akbarwildan@gmail.com

or individuals. Several AI programs, such as Midjourney, Copilot, AI Studio, Prompts, and Dall-E, are responsible for generating much of this fake news. Correcting false information is a focus for some state-run media outlets, and online news sites sometimes take similar action.

Elhoussainy (2024) revealed that political news, particularly news about the government, is the most frequently faked, particularly during times of political turmoil. This misinformation is often disseminated to support government objectives, garner public support, and serve the interests of specific political parties or individuals. Several AI programs, such as Midjourney, Copilot, AI Studio, Prompts, and Dall-E, are responsible for creating much of this fake news. Correcting false information is a matter of interest for some state media outlets, and online news sites sometimes take similar action. In the context of social media, Facebook and YouTube are the most popular platforms for spreading false information, especially fake photos, which are the most common element that spreads quickly (Kumar & Taylor, 2024).

Furthermore, artificial intelligence techniques contribute to the amplification of fake news because some AI techniques are easily applied to fake photos. Fake news also fuels electoral violence, ethnoreligious conflict, distrust of leadership, and injustice. Therefore, genuine news needs to be disseminated in the media to raise awareness of the dangers of using artificial intelligence technology. Strict laws and legislation penalizing news fabrication are needed, as well as the use of fact-checking techniques to combat fake news (Elhoussainy, 2024). Currently, we see numerous photos and videos of politicians and prominent figures fabricated, all of which are the result of the use of artificial intelligence techniques, which can impact national security. Technological developments, the digital revolution, and the emergence of social media platforms have opened up spaces for users to discuss and debate news, and the emergence of artificial intelligence techniques has facilitated the widespread dissemination of fake news. Furthermore, according to Elhoussainy (2024), there is a significant correlation between the level of use of artificial intelligence in news fabrication and its impact on national security.

AI technology not only facilitates the mass production of fake content but also strategically targets vulnerable audiences using micro-targeting techniques and user behavior analysis (Kertysova, 2018). For example, AI can leverage personal data to craft narratives designed to influence the perceptions of specific individuals or groups, as seen in the misuse of deepfakes for political propaganda or social conflict (Jain, 2023).

In the defense context, the dissemination of AI-based disinformation is increasingly recognized as an effective form of non-conventional warfare. Sophisticated disinformation campaigns can be deployed by state and non-state actors to attack political institutions, undermine government legitimacy, and create social instability without requiring direct military intervention (Burton & Soare, 2019). For instance, some nations have employed AI to spread propaganda aimed at disrupting election processes or eroding public trust in democratic institutions (Okolo, 2024).

AI-based disinformation also presents significant challenges in detection and mitigation. While AI technologies can be used to detect disinformation, the effectiveness of such systems remains limited by technical challenges, such as biased training data and the rapid evolution of technology, which allows new algorithms to evade detection (Santos, 2023). Furthermore, ethical concerns, such as freedom of expression and the risk of technology misuse, must be considered when developing mitigation strategies (Hasimi & Poniszewska-Marańda, 2024).

The dissemination of AI-based disinformation has demonstrated its impact in the geopolitical context, including how certain state actors use this technology to weaken their adversaries through information warfare. For example, politically and socially driven conflicts fueled by disinformation have been reported to affect national stability in various countries, including the United States, where election manipulation remains a major concern (Landor-Murray et al., 2019).

This study aims to explore the strategic implications of AI in the dissemination of disinformation, particularly its impact on information security and national defense strategies. Through a literature review and case study analysis approach, this research seeks to provide a comprehensive understanding of the strategic threats posed by AI technology in the defense context, as well as the mitigation measures required to strengthen resilience against such threats.

Method

This study employs a combination of qualitative and quantitative approaches to explore how artificial intelligence (AI) is used in the dissemination of disinformation and its impact on defense strategies. The qualitative approach focuses on a literature review to understand the latest developments in AI-based disinformation detection technologies. This review includes an analysis of detection techniques such as algorithms based on Natural Language Processing (NLP), machine learning, and deep neural network models. For instance, [Karinshak & Jin \(2023\)](#) developed a conceptual framework to identify risks and respond to AI-based disinformation attacks within organizational contexts. They emphasized the need for comprehensive mitigation strategies, including the integration of AI detection systems and the training of communication teams to enhance organizational resilience against false information threats ([Karinshak & Jin, 2023](#)).

A study by [Vysotska \(2024\)](#) expands on this approach by evaluating the effectiveness of machine learning models in recognizing propaganda at both document and sentence levels. This approach includes leveraging algorithms such as TF-IDF, the Bag of Words model, and Word2Vec to generate word vector representations used in propaganda classification. Their research indicates that document-level machine learning models outperform sentence-level models, achieving an accuracy score of 94.3% ([Vysotska, 2024](#)).

The quantitative approach involves the development and evaluation of AI-based models designed to detect disinformation across various formats, including text, images, and video. Data is collected from various social media platforms using scraping techniques, which include textual content, metadata, and visual elements such as videos and images. Adaptive analysis techniques are employed to track patterns in the distribution of false information and its sources.

[Lai & Guo \(2024\)](#) highlight the importance of adaptive analysis in identifying links between disinformation sources and their distribution networks. They developed a framework capable of recognizing disinformation distribution patterns through content analysis and URL metadata, yielding significant results in distinguishing fake information clusters from authentic ones ([Lai & Guo, 2024](#)).

The detection models used in this research are evaluated using metrics such as accuracy, precision, recall, and F1 score to ensure reliability. These evaluations refer to a meta-analysis by [Kozik et al. \(2024\)](#), which compared the performance of various AI-based fake news detection methods. Their study offers insights into the effectiveness of NLP-based approaches, including convolutional neural network (CNN) algorithms and bidirectional LSTM, in detecting fake news across diverse datasets. They found that a combination of CNN and LSTM models achieved the best performance, with the highest F1 score among other approaches ([Kozik et al., 2024](#)).

Through this mixed-method approach, the study not only provides theoretical insights but also practical applications for understanding and addressing AI-based disinformation threats. By leveraging machine learning models, adaptive analytical techniques, and data-driven evaluations, this research lays the groundwork for developing more robust defense strategies against false information attacks generated by AI.

Results and Discussion

This research reveals that artificial intelligence (AI) has a significant impact on the dissemination of disinformation, with far-reaching implications for social stability, economic security, and national defense. One of the key findings is the increased scale and efficiency of AI-based attacks, such as automated disinformation and deepfakes. AI enables the creation of deceptive content that is difficult to distinguish from the truth, often used in information manipulation campaigns to influence public opinion and strategic decision-making. For instance, a study by [Karthikeyan \(2024\)](#) found that AI has been employed to enhance cyberattack capabilities through machine learning algorithms that exploit user behavior patterns to generate content tailored for specific audiences ([Karthikeyan, 2024](#)).

In the defense context, the research highlights AI's role in accelerating intelligence analysis and supporting strategic decision-making. Applications include real-time data-driven threat detection

and the development of autonomous weapon systems designed to improve military efficiency. [Ahmad et al. \(2021\)](#) emphasized that countries such as the United States and China have adopted AI-based systems in military operations to bolster their strategic competitiveness on the global battlefield ([Ahmad et al., 2021](#)). However, the adoption of such technologies also introduces new risks, including potential misuse in asymmetric conflicts.

In the social and economic domains, the findings indicate that AI-based disinformation can directly undermine political and economic stability. Research by [Karaş \(2024\)](#) demonstrated that AI-driven disinformation affects consumer behavior, erodes trust in business institutions, and triggers financial market volatility. For example, fake news propagated on social media has been shown to damage the reputation of major corporations and influence investor decision-making, resulting in long-term impacts on economic stability ([Karaş, 2024](#)).

Additionally, this study underscores advancements in AI-based fake news detection technologies, which have shown promising results in identifying disinformation across various platforms. Machine learning models such as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks have achieved detection accuracy rates of up to 94%, as reported by [Paredes \(2023\)](#). However, despite their effectiveness, these technologies face challenges such as data bias and adaptability to diverse informational contexts ([Paredes, 2023](#)).

The study also reveals that AI amplifies disinformation campaigns during critical political events, such as elections. [Okolo \(2024\)](#) observed that the use of AI-driven disinformation in the electoral context in Africa has fostered distrust in democratic processes, influenced election outcomes, and even sparked significant social tensions ([Okolo, 2024](#)). This demonstrates how AI can serve as a powerful tool in bolstering national defense systems, but also poses a severe threat when used for destructive purposes.

Overall, the findings of this study confirm that AI is a double-edged sword—it can strengthen national defense through enhanced threat detection systems and strategic decision-making but can also become a significant threat when misused. These findings provide a strong foundation for developing more effective mitigation policies and regulations to address the challenges posed by AI in the spread of disinformation.

Discussion

Artificial intelligence (AI) has emerged as a double-edged sword in the context of defense and information security. On one hand, AI enhances the efficiency and capability of threat detection systems; on the other hand, it introduces new risks through the misuse of technology for spreading disinformation. This discussion delves deeper into these impacts, including the challenges, opportunities, and mitigation strategies that can be implemented.

AI has significantly improved disinformation management, particularly in the automated detection of fake news using machine learning algorithms and natural language processing (NLP). Models like convolutional neural networks (CNNs) and long short-term memory (LSTM) networks have demonstrated their effectiveness in identifying suspicious linguistic patterns, often characteristic of fake news ([Paredes, 2023](#)). However, technical challenges such as training data bias and model adaptation to new contexts remain major obstacles. Further research is needed to develop more flexible algorithms that can adapt to the ever-evolving dynamics of disinformation.

Beyond detection, AI accelerates intelligence analysis capabilities in the defense sector. The technology enables faster decision-making through real-time analytics and big data processing. For example, AI-based systems have been adopted to detect cyber threats and identify sources of false information disseminated on digital platforms. A study by [Radovanović et al. \(2024\)](#) highlights the use of AI-powered drones in military operations to provide tactical advantages through autonomous data collection and adaptation to battlefield conditions ([Radovanović et al., 2024](#)). However, the use of AI in the military also introduces strategic risks, such as the potential misuse of technology for offensive purposes in cyber warfare.

In social and political domains, AI has transformed the dissemination of disinformation, particularly in the context of elections and democratic processes. Research by [Okolo \(2024\)](#) illustrates how AI-driven disinformation campaigns have been used to manipulate public opinion in Africa, fostering distrust in democratic institutions and even inciting social conflict ([Okolo, 2024](#)). These

strategies demonstrate that disinformation not only undermines public trust but can also disrupt political and social stability on a large scale. Globally, this poses new challenges for governments and international organizations to develop stricter regulatory strategies to control AI use in politics.

In the economic sector, AI-based disinformation has inflicted significant damage on companies and financial markets. Karaş (2024) found that fake news can erode consumer trust in brands, influence investment decisions, and trigger financial market volatility (Karaş, 2024). Companies must invest more in AI technologies to protect their reputations and mitigate the effects of disinformation, which can severely undermine market confidence.

The discussion also emphasizes the need for a multidimensional approach to address the challenges of AI-driven disinformation. Collaboration among governments, the private sector, and civil society is crucial in building resilience against these threats. For instance, improving public digital literacy can help reduce the impact of fake news by educating people on how to recognize disinformation. This aligns with a study by Sharma (2023), which highlights the importance of integrating AI technology with manual training to balance technological efficiency with human intuition in addressing cyber threats (Sharma, 2023).

From a policy perspective, the discussion underscores the importance of international regulations to prevent the misuse of AI in spreading disinformation. Cai & Zhang (2024) propose that major nations like the United States and China should lead global efforts to establish ethical frameworks and regulations governing AI use in military and political contexts (Cai & Zhang, 2024). This would involve enforcing laws against the use of AI for destructive purposes and forming international alliances to address cross-border threats.

In conclusion, this discussion reaffirms that AI is an immensely powerful tool but is vulnerable to misuse. Its success as a tool for defense and threat mitigation depends on the implementation of prudent policies, the responsible development of technology, and effective global collaboration to create a safer digital world.

According to Deepak (2023), within the context of the media ecosystem, within the propagation segment, we observe that the logic of the attention economy prioritizes disinformation through various pathways, including those aligned with current understandings of human psychology. Turning to mitigation, a segment often presented as one where AI can play a meaningful and positive role, we analyze the current AI paradigm and its operational modalities. Critically analyzing AI in this context. Furthermore, the differences in decision-making styles between humans and AI can have significant consequences in the realm of fake news.

According to Nasiri & Hashemzadeh (2025), AI-generated misinformation, particularly deepfakes, is becoming increasingly difficult to detect, even by sophisticated AI systems. The implications of this shift for democratic processes, public trust, and social cohesion are profound. Furthermore, according to the two, as AI technology advances, the threat posed by AI-based disinformation is becoming increasingly acute, demanding a multifaceted response from technologists, policymakers, academics, and the wider public. AI has enabled the mass production and dissemination of disinformation on a previously unimaginable scale, eroding trust in the media, eroding democratic processes, and sowing divisions in society. This aligns with information noise theory and information quality theory. Referring to information noise theory, these forms of information noise become even more potent when amplified by AI technology. AI can automate the creation and dissemination of misinformation and disinformation, often increasing their reach and effectiveness. The danger lies not only in the scale and speed with which AI disseminates false information, but also in the personalization and contextualization of content to target specific audiences. From the perspective of information quality theory, information noise is seen as a failure of information quality; this approach underscores the need for systems that filter and prioritize content based on trust signals. Social media platforms must adopt algorithms that amplify high-quality content while deprioritizing harmful or misleading narratives.

Furthermore, within the framework of a defense strategy, as Kaczmarek, Karpiuk & Melchior (2024) argue, society is unaware of the influence of hostile information that some actors seek to wield. Awareness of disinformation processes remains low, as is the level of practical solutions implemented in the information sphere. Building and developing social resilience to disinformation is crucial,

especially in times of cognitive warfare spread by hostile global actors. The greater the polarization within society, the lower the level of education, and the less critical thinking used to absorb knowledge from the infosphere, the more easily the nation is influenced and pushed into certain actions. To remain aware of reality and develop conscious and healthy multidimensional social relationships, society must be equipped with the tools to survive and supported by the state in the fight against information threats. Combating disinformation is a crucial element in creating and strengthening social resilience against hostile information operations in times of cognitive warfare.

Conclusion

This research demonstrates that artificial intelligence (AI) has a significant impact on the dissemination of disinformation, with far-reaching implications for social stability, economic security, and national defense. On one hand, AI serves as an extremely effective tool for bolstering defense through advanced threat detection, real-time data analytics, and enhanced military strategies. On the other hand, it becomes a threat when used to create disinformation that is difficult to distinguish from the truth, undermining public trust, manipulating political processes, and inciting social conflict.

In the defense context, this study highlights how AI has accelerated the development of autonomous military systems and improved strategic decision-making, though it also introduces new strategic risks, such as the misuse of technology by malicious actors. In social and political spheres, AI is employed to orchestrate disinformation campaigns designed to sway public opinion and create political instability. Economically, the effects include significant financial losses due to market manipulation and diminished consumer trust in business institutions.

To address these challenges, a multidimensional approach involving collaboration among governments, the private sector, and civil society is essential. Key measures include improving digital literacy, developing more sophisticated disinformation detection technologies, and establishing strict international regulations. This study emphasizes that success in leveraging AI responsibly will depend heavily on prudent policymaking, robust ethical frameworks, and global cooperation to create a safer and more sustainable digital environment.

In conclusion, AI is a double-edged sword that offers immense benefits for defense and global security but also poses significant risks if not properly managed. Therefore, responsible technological development and cross-sector collaboration are critical to ensuring that AI is harnessed to enhance stability, security, and societal well-being.

References

- Azam, A. (2021). Role Of Artificial Intelligence In Defence Strategy: Implications For Global And National Security. *Strategic Studies*. <https://doi.org/10.53532/Ss.041.01.0058>.
- Benzie, A., & Montasari, R. (2022). Artificial Intelligence And The Spread Of Mis-And Disinformation. In *Artificial Intelligence And National Security* (Pp. 1-18). Cham: Springer International Publishing.
- Burton, J., & Soare, S. (2019). Understanding The Strategic Implications Of The Weaponization Of Artificial Intelligence. 2019 11th International Conference On Cyber Conflict (Cycon), 900, 1-17. <https://doi.org/10.23919/CYCON.2019.8756866>.
- Cai, C., & Zhang, L. (2024). Escaping The Trap: Adapting The U.S.-China Arms Race To The Dynamics Of Artificial Intelligence. *North South Journal Of Peace And Global Studies*. <https://doi.org/10.47126/Nsjpgs.V2i1.02>.
- Deepak, P. (2023). AI And Fake News: Unpacking The Relationships Within The Media Ecosystem. *Communication & Journalism Research*, 12(1), 15-32.
- Elhoussainy, H. A. (2024). The Role Of Artificial Intelligence Techniques In Spreading Rumors And Fake News, And Their Effect On National Security, 2024(30), 1-59.
- Gaire, U. (2023). Application Of Artificial Intelligence In The Military: An Overview. *Unity Journal*. <https://doi.org/10.3126/Unityj.V4i01.52237>.
- Hasimi, L., & Poniszewska-Marańda, A. (2024). Detection Of Disinformation And Content Filtering Using Machine Learning: Implications To Human Rights And Freedom Of Speech. *ROMCIR@ECIR*.

- Jain, R. (2023). Detection And Provenance: A Solution To Deepfakes?. *Journal Of Student Research*.
<https://doi.org/10.47611/jsrhs.v12i3.5122>.
- Kaczmarek, K., Karpiuk, M., & Melchior, C. (2024). Disinformation As A Threat To State Security. *Przegląd Nauk O Obronności*, 9(20), 45-54.
- Karaş, Z. (2024). Effects Of AI-Generated Misinformation And Disinformation On The Economy. *Düzce Üniversitesi Bilim Ve Teknoloji Dergisi*.
- Karinshak, E., & Jin, Y. (2023). AI-Driven Disinformation: A Framework For Organizational Preparation And Response. *Journal Of Communication Management*.
<https://doi.org/10.1108/jcom-09-2022-0113>.
- Karthikeyan, S. (2024). Rising Threat Of AI-Driven Cybersecurity Attacks: Implications For National Security. *International Journal For Research In Applied Science And Engineering Technology*.
<https://doi.org/10.22214/ijraset.2024.64042>.
- Kertysova, K. (2018). Artificial Intelligence And Disinformation. *Security And Human Rights*.
<https://doi.org/10.1163/18750230-02901005>.
- Kozik, R., Pawlicka, A., Pawlicki, M., Choraś, M., Mazurczyk, W., & Cabaj, K. (2024). A Meta-Analysis Of State-Of-The-Art Automated Fake News Detection Methods. *IEEE Transactions On Computational Social Systems*, 11, 5219-5229.
<https://doi.org/10.1109/TCSS.2023.3296627>.
- Kumar, A., & Taylor, J. W. (2024). Feature Importance In The Age Of Explainable AI: Case Study Of Detecting Fake News & Misinformation Via A Multi-Modal Framework. *European Journal Of Operational Research*, 317(2), 401-413.
- Lai, C., & Guo, Y. (2024). Tracking Of Disinformation Sources: Examining Pages And Urls. *IEEE Transactions On Computational Social Systems*, 11, 6242-6253.
<https://doi.org/10.1109/TCSS.2024.3391626>.
- Landon-Murray, M., Mujkic, E., & Nussbaum, B. (2019). Disinformation In Contemporary U.S. Foreign Policy: Impacts And Ethics In An Era Of Fake News, Social Media, And Artificial Intelligence. *Public Integrity*, 21, 512 - 522.
<https://doi.org/10.1080/10999922.2019.1613832>.
- Nasiri, S., & Hashemzadeh, A. (2025). The Evolution Of Disinformation From Fake News Propaganda To AI-Driven Narratives As Deepfake. *Journal Of Cyberspace Studies*, 9(1), 229-250.
- Nazar, S., & Bustam, M. R. (2020, July). Artificial Intelligence And New Level Of Fake News. In *IOP Conference Series: Materials Science And Engineering* (Vol. 879, No. 1, P. 012006). IOP Publishing.
- Okolo, C. (2024). African Democracy In The Era Of Generative Disinformation: Challenges And Countermeasures Against AI-Generated Propaganda. *Arxiv*, Abs/2407.07695.
<https://doi.org/10.48550/Arxiv.2407.07695>.
- Paredes, D. (2023). Strategies Based On Artificial Intelligence For The Detection Of Fake News. *AWARI*. <https://doi.org/10.47909/Awari.58>.
- Radovanović, M., Petrovski, A., Behlić, A., Chaari, M. Z., Hashimov, E., & Fellner, R. (2024). Unleashing Autonomous Forces: Integrating AI-Driven Drones In Modern Military Strategy. *Системи Управління, Навігації Та Зв'язку*.
- Santos, F. (2023). Artificial Intelligence In Automated Detection Of Disinformation: A Thematic Analysis. *Journalism And Media*. <https://doi.org/10.3390/Journalmedia4020043>.
- Shoaib, M., Wang, Z., Ahvanooe, M., & Zhao, J. (2023). Deepfakes, Misinformation, And Disinformation In The Era Of Frontier AI, Generative AI, And Large AI Models. *Arxiv*, Abs/2311.17394. <https://doi.org/10.48550/Arxiv.2311.17394>.
- Vysotska, V. (2024). Information Technology For Recognizing Propaganda, Fakes And Disinformation In Textual Content Based On Nlp And Machine Learning Methods. *Radio Electronics, Computer Science, Control*. <https://doi.org/10.15588/1607-3274-2024-2-13>.

