SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 01 No. 02 (2024), pp. 122-127
Research Article
doi: https://doi.org/10.70710/sitj.v1i2.16

Utilization of Artificial Intelligence in Monitoring and Mitigating National Security Threats

Angga Junior Wiranata[1,a,*]

[1]Sekolah Tinggi Intelijen Negara
[a]anggaaarum@gmail.com
*Corresponding author

Article Info
Received: 13-Nov-2024
Revised: 20-Nov-2024
Accepted: 01-Dec-2024

Keywords
Artificial Intelligence; National Security; Socio-Technical Systems

Abstract
Implementing Artificial Intelligence (AI) in the context of national security has become a critically important topic in addressing increasingly complex modern threats. This article examines various AI applications in monitoring and mitigating national security threats, such as managing critical infrastructure, risk assessment, and adaptive responses to crises. By adopting the socio-technical systems theory approach, this approach recognizes the complexity of interactions between AI technology, human decisions, and operational environments that impact national security. Recommendations include increased investment in advanced AI infrastructure and more profound training for AI and the national security workforce. It is expected that mature AI implementation can significantly impact maintaining stability and national security in this dynamic digital era.

1. Introduction

Artificial Intelligence (AI) is a computer science discipline that aims to create systems or machines capable of performing tasks that generally require human intelligence, including learning from data, recognizing patterns, making decisions, and understanding natural language. In recent decades, AI advancements have accelerated significantly, with applications ranging from autonomous vehicles to virtual assistants like Siri and Google Assistant. AI has proven to enhance efficiency and effectiveness in numerous sectors.

The development of AI began in the 1950s when John McCarthy, Marvin Minsky, and other MIT scientists formed a research group to explore these concepts. They developed computer programs mimicking human abilities, such as processing natural language and playing chess. The early peak of AI development occurred in 1956 with McCarthy's Dartmouth Conference, a crucial turning point that established AI as an independent field. Despite stagnation in the 1970s due to technical and financial challenges, AI experienced rapid progress in the 1980s alongside advances in computer technology. Another significant achievement was in 1997 when IBM's Deep Blue computer program defeated world chess champion Garry Kasparov. In the last decade, AI advancements have become even more meaningful with the development of deep learning technology and artificial neural networks, enabling computers to learn from data and improve performance autonomously. Today, AI is embedded in various applications such as autonomous vehicles, voice and facial recognition, and virtual assistants (Kemenkeu, 2023).

AI development has become a cornerstone in modern technology, evolving from concept development in the 1950s to its peak today with deep learning and neural network technology. AI changes how we interact with everyday technology, such as through virtual assistants and autonomous vehicles, and opens new opportunities across various sectors, including national security. In national security, AI holds significant potential to strengthen monitoring and mitigation capabilities against threats ranging from

cyber-attacks to transnational crime. By leveraging in-depth data analysis and high predictive capabilities, AI can detect, analyze, and respond to threats more quickly and efficiently than conventional approaches. However, while pursuing this potential, it is important to consider ethical challenges, data security, and policies related to AI applications in national security.

National Security can be understood both as a condition and as a function. As a function, National Security aims to create and maintain a broad sense of safety, encompassing feelings of comfort, peace, calm, and order. Such security and well-being are fundamental human needs. Understanding the meaning and substance of National Security varies depending on the values, perceptions, and interests involved (Wantannas). We can see how AI can reinforce these aspects by understanding National Security as a condition and function aimed at creating a sense of security, comfort, peace, calm, and order. With its deep data analysis and predictive response capabilities, AI offers innovative solutions for monitoring and countering security threats. For instance, AI can detect cyber-attacks in real time, identify threat patterns before they become critical, and coordinate responses to physical and digital threats more efficiently than traditional methods. Additionally, AI applications in National Security can aid in crisis management and disaster recovery, ensuring a sense of security and comfort is maintained during challenging situations. However, AI must always be accompanied by ethical considerations and appropriate policies to prevent misuse and ensure its application genuinely benefits public security and welfare.

The background of this research is driven by the increasing frequency and complexity of threats to national security, especially those originating from cyber-attacks. Critical infrastructure, such as power grids, transportation systems, and healthcare facilities, often becomes primary targets for cyber-attacks, leading to significant losses and threatening national stability. Moreover, rapid developments in AI offer potential solutions for monitoring and mitigating these threats more effectively and efficiently. AI can analyze large volumes of data, detect suspicious patterns, and respond to threats in real-time, helping maintain critical infrastructure's integrity and security. Therefore, this study explores how AI can be optimally implemented to strengthen national security in this digital era.

Although AI has great potential to enhance national security, its application still faces several challenges. These challenges include the need for large, high-quality datasets to train AI algorithms and concerns regarding privacy and data security. The risk of errors or biases within AI systems is also a concern. Adopting AI technology in the security sector requires substantial investment, infrastructure, and human resource readiness. The research problem addressed in this study is how AI can effectively monitor and mitigate national security threats. This study aims to examine AI applications in the context of national security, analyze the benefits and challenges faced, and provide recommendations for improved implementation. Thus, this research is expected to significantly contribute to developing a national security strategy that is more adaptive and responsive to modern threats.

2. Methods

The method used in this study is a literature review, in which the author searches for and interprets sources from various literature using a scientific approach and a descriptive qualitative or naturalistic method, as this research is conducted in a natural setting. In his book, "Research Methods," M. Nazir explains that a literature review is a data collection technique involving examining books, literature, records, and reports related to the problem. This method enables researchers to gather relevant information, build a solid theoretical foundation, and provide broader and deeper insights into the research topic (Nazir, 1988). To write a scientific journal titled "Utilization of Artificial Intelligence in Monitoring and Mitigating National Security Threats," the appropriate theory is the "Socio-Technical Systems Theory." This theory emphasizes the interaction between humans, technology, and the environment within the broader context of organizations or systems, making it highly relevant to the application of AI in the field of national security.

The Socio-Technical Systems Theory stresses that a balance between social and technical aspects within an organization is essential for achieving effectiveness. Applying AI in national security requires a deep understanding of how this technology will interact with social factors such as policies, procedures, and human resource readiness. Therefore, the effectiveness of AI does not depend solely on the technology itself but also on how it is adopted and utilized by humans within a specific work environment (Chern, 1976). In this context, the Socio-Technical Systems Theory helps researchers explore how AI can be optimally implemented within national security systems by considering the interaction between

technology and social factors. For example, AI can analyze large volumes of data, detect threat patterns, and provide rapid responses. However, strong integration between AI systems and security teams and policies supporting this technology is needed to maximize its effectiveness.

3. Result and Discussion

Article 1, Paragraph 4 of the Republic of Indonesia Law Number 17 of 2011 refers to the definition of a threat as follows:

> "Ancaman adalah setiap upaya, pekerjaan, kegiatan, dan tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan."

The definition of a "threat" in Article 1, Paragraph 4 of Indonesian Law Number 17 of 2011 encompasses any effort, work, activity, or action, whether domestic or foreign, that is deemed or proven to endanger national safety, security, sovereignty, territorial integrity, or national interests. This includes potential harm across various aspects, including ideology, politics, economy, socio-culture, defense, and security.

Barry Buzan (1983) categorized security threats into five main sectors based on the affected sector. This categorization includes military, political, social, economic, and ecological threats. Military threats are the potential for military attacks or invasions that can disrupt a nation's sovereignty and safety. Political threats are related to internal tensions, such as coups or internal conflicts that can destabilize political stability. Social threats encompass disputes between ethnic, religious, or social groups that can spark unrest or large-scale conflict. Economic threats include economic crises or international sanctions that could damage national economic stability. Ecological threats involve natural disasters or environmental changes that threaten the sustainability of ecosystems and human welfare.

The evolution of modern times indicates that the nature of threats has transformed into complex and multi-dimensional forms, where competition and conflicts between nations often lead to types such as proxy wars, hybrid warfare, or gray zone conflicts. On the other hand, Robert Ring has categorized threats into four levels: minor, moderate, severe, and critical (Soekarno, 2014). Hank Prunckun (2010), in his book "Handbook of Scientific Methods of Inquiry for Intelligence Analysis," defines threats as the intent or desire of individuals, organizations, or countries to cause harm or damage to various entities, such as individuals, organizations or states, whether in explicit or hidden forms. In threat analysis, two main factors are considered: the identity of the threat actor, which could be an individual, group, or state, and the target of the threat, which includes various aspects of national security, whether physically observable or not.

The views on threat definitions and classifications presented by various researchers and laws reflect the complexity of threats today. The Republic of Indonesia Law Number 17 of 2011 defines national safety, security, sovereignty, and national interests in various aspects of life. Barry Buzan's and Robert Ring's perspectives offer classifications and levels of threat severity. At the same time, Hank Prunckun emphasizes the intent and desire of entities to cause harm or damage, which is essential in understanding threats in an intelligence context. These perspectives highlight the need for a multidimensional approach and dynamic adaptation in identifying, assessing, and addressing threats in an increasingly complex and rapidly changing world.

Current Threat

Current threats are becoming increasingly complex, with various factors that can threaten national stability, especially in the context of social changes, technology, and global security. One of the threats that needs to be watched out for is the development of transnational criminal networks, including drug trafficking, which is growing globally. Organizations such as the Sinaloa Cartel and the Jalisco Cartel, based in Mexico, continue to expand their influence by exploiting smuggling routes and increasingly sophisticated drug production, including dangerous substances like fentanyl. The rising number of drug smuggling incidents mixed with other harmful substances, such as xylazine (tranq), complicates efforts to combat overdoses, which poses a severe threat to public health and national safety (WE Forum, 2024).

Additionally, the threat from disinformation campaigns initiated by adversarial nations has become increasingly apparent. Countries like Russia, China, and Iran are actively using media and digital platforms to spread narratives that threaten the social and political resilience of other nations. Misinformation, disinformation, and malinformation spread in a structured manner aim to weaken public trust in government institutions and disrupt the democratic process. The use of new technologies, including AI, to create high-quality fake content further exacerbates this situation. Considering its impact on social and political stability, this creates a significant challenge for national resilience (Homeland Security, 2024).

Responding with a holistic and coordinated approach is essential in addressing these challenges. Laws and theories that have been put forward, such as Barry Buzan's views on the classification of threats and Robert Ring's concept of the seriousness of threats, provide a framework for understanding and evaluating the complexity of modern threats. Meanwhile, the socio-technical systems theory applied in the context of AI can be an innovative solution for monitoring and mitigating these multidimensional threats. The application of AI technology in data analysis and predictive responses can enable early detection, in-depth analysis, and quick responses to threats that may undermine national security. Therefore, integrating advanced technology with a multidimensional approach to national security is crucial in facing the current global era's increasingly complex and dynamic challenges.

Types of AI

Here are some examples of AI applications that can be effectively used to detect, monitor, and address national threats:

a. **Real-Time Anomaly Detection**: AI can analyze network traffic and user activity to detect unusual patterns and potential threats in real time. This technology allows systems to detect previously unseen attacks by monitoring deviating behaviors, whether from users or the system itself. For example, AI can identify unauthorized access or suspicious data transfers on protected systems (SecureTrust, 2024).

b. **Predictive Analytics for Threat Intelligence**: AI can predict potential threats or vulnerabilities using historical data. This helps organizations prioritize the most significant threats so that preventive actions can be taken earlier. For instance, by analyzing data from previous attacks, AI can map patterns that assist in forecasting future threats, enabling faster and more efficient responses (DataCorps, 2023).

c. **Incident Response Automation**: AI can automate threat analysis processes and respond more quickly when facing cyberattacks. For example, AI-powered systems can identify ransomware attacks and immediately isolate infected systems to prevent further spread. This technology effectively minimizes the damage caused by fast and widespread cyberattacks (SecureTrust, 2024).

d. **Phishing Detection and Endpoint Security**: AI can also detect phishing emails by analyzing the content, sender, and URLs in suspicious emails. AI can provide better protection against these threats by identifying patterns associated with previous phishing attacks. Additionally, AI can monitor endpoint devices for signs of suspicious activity, such as file modifications or unauthorized access, to prevent malware or ransomware attacks (DataCorps, 2023).

Implementation

Implementing AI in national threat mitigation has evolved into an integral approach within national security systems. In this approach, AI detects and responds to threats automatically through deep data and behavioral analysis. Technologies such as real-time anomaly detection enable systems to identify suspicious activities, such as unauthorized data transfers or illegal access, so preventive actions can be taken immediately. AI can also identify and anticipate attack patterns that have never occurred before, functioning as a shield that continuously adapts to various threats. This implementation aligns with the socio-technical systems theory, which emphasizes the interaction between technology and humans, where the role of AI not only replaces but also strengthens human capabilities in monitoring and addressing threats effectively.

Additionally, applying AI-based predictive analytics becomes an essential tool for threat intelligence to identify potential attacks before they occur. By utilizing historical data from previous threats, AI can develop predictive patterns that alert security forces about future threats, allowing proactive decisions to be made before the situation becomes critical. This reflects the interaction between humans and technology that supports each other in socio-technical systems, where AI acts as a tool to enrich human analysis and decision-making. When threats are successfully predicted, mitigation actions will be more focused and can reduce the risk impact on national security.

AI also provides advantages in automated incident response, mainly when dealing with attacks that require quick action, such as ransomware. Once an attack is detected, AI can isolate infected systems to prevent further spread, providing a much faster response than manual actions. This implementation integrates technology systems with human security policies, which aligns with socio-technical theory, which views technology as an inseparable part of the overall organizational system. Implementing AI creates a more resilient and adaptive national security system that can face continuously evolving threats when supported by a coordinated strategy.

4. Conclusion

The utilization of AI in national threat mitigation is increasingly crucial in the era of globalization and rapid technological advancement. AI provides the capability to detect, monitor, and respond to threats efficiently through real-time and predictive data analysis, enabling preventive actions before threats escalate. AI systems like those used in anomaly detection and predictive analytics demonstrate optimal synergy between humans and technology. This implementation strengthens security systems through faster responses and higher precision compared to manual methods, which aligns with socio-technical systems theory, which harmonizes technological aspects with the role of humans.

Through predictive analytics and automated response concepts, AI can process and interpret data from various sources to generate insights relevant to potential threats. This enables security forces to mitigate risks more effectively and efficiently. With AI's pattern analysis capabilities, cyber and physical threats can be predicted more accurately, which in turn helps authorities design better strategies to prevent attacks. This ability reflects the importance of AI in enhancing the role of humans as decision-makers, making it a crucial component of a socio-technical system responsive to modern threats' development.

Furthermore, the application of AI in incident response automation becomes an effective solution in facing threats that require swift action, such as ransomware attacks. AI technology can identify attacks and automatically take isolated actions to prevent broader impacts. This shows that the role of AI is not merely as an aid but as an integral part of the national security system. This system helps accelerate responses, reduce vulnerability to threats, and directly strengthens national resilience amid increasingly complex threats. However, it is essential to note that implementing AI in national threat mitigation must be balanced with clear regulations and a responsible, ethical approach. Ethical challenges in AI implementation, such as data privacy and the potential for misuse, must be addressed with adequate policies to ensure this technology does not compromise individual rights and human values. Thus, AI can be used effectively and safely to maintain the stability and security of the nation without introducing new risks in the social or political realms.

The appropriate use of AI in line with socio-technical principles enables the creation of a more adaptive, responsive, and sustainable security system. AI adds significant value to data analysis and threat response, contributing to a safer environment at the national level. The practical application of this technology, supported by regulations and multidisciplinary collaboration, will form the foundation for addressing increasingly complex national security challenges in the future.

References

Cherns, A. (1976). "The Principles of Sociotechnical Design." Human Relations, 29(8), 783-792.

Duncan, S., et al. (2020). Artificial Intelligence for Disaster Response and Relief Operations: Challenges, Opportunities, and a Proposed Framework. IEEE Transactions on Engineering Management.

Jin, X., et al. (2017). Social Media Analytics for Natural Disaster Management. IEEE Intelligent Systems.

Koerich, A. L., et al. (2021). Artificial Intelligence Techniques for Disaster Management: A Review. IEEE Access.

Lary, D. J., et al. (2018). Utilizing AI and Machine Learning for Disaster Management. IEEE Access.

Lee, K., et al. (2019). AI Applications in Disaster Response and Management: A Survey. ACM Computing Surveys.

Nazir, M. (1988). Metode Penelitian. Jakarta: Ghalia Indonesia.

Prunckun, Hank. (2010). Handbook of Scientific Methods of Inquiry for Intelligence Analysis. United Kingdom: Scarecrow Press.

Soekarno, Irawan. (2014). Ilmu Intelijen. Sentul: STIN Press.

https://www.djkn.kemenkeu.go.id/kpknl-bandaaceh/baca-artikel/16443/Artificial-Intelligence.html, diakses pada 11 Juli 2024, pukul 10:41 WIB.

https://www.wantannas.go.id/storage/buku/kamnas-wantannas.pdf, accessed on July 11, 2024, at 10:52 AM.

https://www.weforum.org/stories/2024/01/ai-disinformation-global-risks/, accessed on November 6, 2024, at 01:45 PM.

https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf, accessed on November 6, 2024, at 01:50 PM.

https://www.datacorps.com/2023/03/17/how-ai-can-help-detect-and-prevent-cyber-threats/, accessed on November 6, 2024, at 02:20 PM.

https://securetrust.io/blog/leveraging-ai-for-threat-detection-and-response/, accessed on November 6, 2024, at 02:50 PM.