SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 04 (2025), pp. 422-437
Research Article
doi: https://doi.org/10.70710/sitj.v2i4.79

Transforming Intelligence Operations in Indonesia: Challenges and Opportunities in the Digital Age

Muhammad Nur Abdul Latif Al Waro'i[1,a,*]

[1]School of Strategic and Global Studies, University of Indonesia, Indonesia
[a]latif.alwaroi46@gmail.com
*Corresponding author

Article Info
Received: 20-Nov-2025
Revised: 21-Nov-2025
Published: 6-Dec-2025

Keywords
Artificial Intelligence (AI), Big Data, Conventional Intelligence, Cybersecurity, Digital Technology, Machine Learning (ML)

Abstract
The digital revolution has transformed global intelligence paradigms, making advanced technology essential for modernizing national security systems. This paper discusses the integration of digital technologies, such as Artificial Intelligence (AI), Machine Learning (ML), big data analytics, and cybersecurity, into Indonesia's intelligence operations. Traditionally, Indonesia's intelligence relied on Human Intelligence (HUMINT) and Signal Intelligence (SIGINT), but the rise of digital threats such as cyberattacks, terrorism, and social media-driven radicalization now demands the adoption of advanced technologies to improve detection and response effectiveness. This study uses a qualitative methodology and conducts an extensive literature review of academic articles, policy reports, and case studies to explore the application of digital technologies in Indonesia's intelligence context. Key findings reveal that, although AI, big data, and other digital tools present significant potential, their integration is hindered by inadequate infrastructure, data privacy and security concerns, and cultural resistance within the intelligence community. The study recommends improving digital infrastructure, strengthening cybersecurity policies, and fostering public-private partnerships and international collaborations to support Indonesia's intelligence modernization efforts. This research emphasizes the need for continued investment in technology and inter-agency cooperation to enhance Indonesia's intelligence capabilities, ensuring that the country is prepared to tackle 21st-century security challenges.

1. Introduction

The digital revolution has fundamentally transformed global intelligence frameworks, making the integration of advanced technologies essential for modernizing national security systems. Key innovations in artificial intelligence (AI), machine learning (ML), big data analytics, and cybersecurity have revolutionized intelligence gathering, analysis, and response mechanisms. These technologies enable intelligence agencies to efficiently process and analyze vast amounts of data in real time, providing faster and more accurate insights into emerging threats. Traditionally, intelligence operations have relied heavily on Human Intelligence (HUMINT) and Signal Intelligence (SIGINT), focusing on direct surveillance and human informants. However, as security threats have become increasingly digital, including cyberattacks, terrorism, and online extremism, there has been a paradigm shift toward digital intelligence practices capable of detecting and mitigating these modern risks (Srivastava, 2023).

Globally, AI and big data analytics have proven effective in enhancing security operations, from real-time threat detection to predictive analytics that can forecast potential dangers before they materialize (Al-Suqri & Gillani, 2022). For countries in the Global South, including Indonesia, the adoption of such technologies is not merely a matter of modernization, but an urgent necessity to address evolving security challenges. The ability of AI and ML to process large datasets swiftly has become crucial in combating the

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

increasing complexity and speed of modern threats, especially given that many of these threats, such as online radicalization and cybercrime, transcend national borders and occur across digital platforms (Fahmi Nooryadi et al., 2025).

Indonesia's traditional intelligence practices have primarily focused on HUMINT and SIGINT, tools that were effective in the past but are insufficient in managing today's complex and fast-paced security challenges. The emergence of digital threats such as cyberattacks, terrorism, and social media-driven radicalization has highlighted the need for more advanced intelligence tools. Therefore, integrating AI, machine learning, and big data analytics is essential for strengthening Indonesia's national security infrastructure and ensuring that the country can keep up with global advancements in intelligence technology. Indonesia's intelligence agencies face several significant challenges in fully integrating digital technologies, such as AI and big data analytics, into their operations. These challenges include outdated infrastructure, cybersecurity risks, regulatory barriers, and ethical concerns. Although digital technologies present substantial opportunities to enhance intelligence capabilities, they also introduce new complexities that must be addressed to maintain national security and public trust.

A primary issue is the underdeveloped digital infrastructure, which hinders the effective deployment of modern intelligence tools. Despite initial efforts to integrate digital solutions, Indonesian intelligence agencies continue to face gaps in computing power, data storage capacity, and secure communication systems. This has been exacerbated by the lack of interoperability between the various digital systems used by different agencies, making it difficult to achieve seamless coordination in intelligence operations (Wulandari et al., 2025). Furthermore, the growing reliance on cloud-based platforms and interconnected systems has raised concerns about cybersecurity. The risks of cyberattacks and data breaches, including the potential for adversaries to intercept sensitive information, have intensified, necessitating stronger safeguards for digital communication and data storage (Ishak, 2023).

Additionally, there is resistance within the intelligence community to adopting digital technologies, particularly because of the deeply ingrained culture of secrecy and hierarchical control. The shift toward a more transparent, collaborative, and technology-driven approach to intelligence work presents significant organizational challenges, such as the need for inter-agency cooperation and alignment of institutional priorities (Nur et al., 2024). Ethical issues, including the potential for AI-driven surveillance to infringe on privacy rights, also remain a key concern as Indonesia moves toward more advanced digital intelligence operations.

This study focuses on the integration of digital technologies into Indonesia's intelligence operations, specifically examining how technologies such as AI, machine learning, big data analytics, and cybersecurity can enhance national security and counterterrorism efforts. The scope of this study includes the evolution of Indonesia's intelligence practices, the challenges faced in integrating digital tools, and the potential opportunities these technologies offer in addressing modern security threats. The key objectives of this study are as follows:

1. To identify the primary challenges faced by Indonesia's intelligence agencies in adopting digital technologies, including infrastructure limitations, cybersecurity concerns, and institutional resistance.
2. To examine the role of AI, big data, and machine learning in enhancing Indonesia's counterterrorism efforts and improving real-time threat detection.
3. To explore the ethical, regulatory, and privacy issues that arise when using digital technologies in intelligence operations.
4. To investigate the potential for public-private partnerships and international collaborations to support Indonesia's intelligence modernization efforts.

This study will provide a comprehensive analysis of how Indonesia can overcome existing barriers and leverage digital tools to improve national security operations.

2. Methodology

This study utilized a qualitative research methodology, relying on an extensive study of the existing literature, including academic articles, policy reports, and case studies, to explore the integration of digital technologies into intelligence operations. Key databases, such as Scopus, JSTOR, and Google Scholar, were

searched to identify relevant studies and reports on the subject. The literature studied includes both global and local perspectives on digital intelligence practices, with a particular focus on AI, machine learning, and big data analytics in intelligence and security contexts. The analysis also incorporates examples of successful digital integration in intelligence agencies worldwide, with an emphasis on the challenges and opportunities faced by Indonesia's intelligence community.

3. Results and Discussion

3.1. The Evolution of Intelligence Operations in Indonesia

Indonesia's intelligence operations have undergone profound transformations since its independence, adapting to the shifting security landscape over decades. Initially relying heavily on traditional methods like Human Intelligence (HUMINT) and Signal Intelligence (SIGINT), the country's intelligence apparatus has evolved significantly to address contemporary security threats, particularly as new challenges emerge in the digital age.

Traditional Intelligence Methods and Practices in Indonesia

Indonesia's intelligence community emerged in the wake of independence, marked by the need to navigate various internal and external threats. Early intelligence operations were deeply intertwined with the state-building process, where control over regional insurgencies, ideological movements, and foreign influences was crucial. HUMINT and SIGINT were the dominant methods of intelligence gathering used to secure Indonesia's sovereignty and prevent any destabilizing elements from threatening national security.

1. The Role of HUMINT and SIGINT

   Human Intelligence (HUMINT) played a pivotal role in Indonesia's intelligence operations, especially during the Sukarno and Suharto eras. Intelligence agencies such as the State Intelligence Agency (BIN) relied on an extensive network of informants, agents, and spies. These human sources were integral in infiltrating insurgent groups, such as communist organizations, and curbing separatist movements. HUMINT allowed for subtle, contextual understanding of political climates, which was essential in times of ideological conflict (Macêdo et al., 2023).

   Alongside HUMINT, SIGINT emerged as a crucial intelligence tool, especially as global communication technologies advanced. In the 20th century, the ability to intercept radio signals, telephone conversations, and satellite communications became vital for monitoring both domestic and foreign threats. During the Cold War, SIGINT allowed Indonesia to keep track of foreign adversaries, and post-9/11, it was pivotal in countering terrorism. For instance, intercepting terrorist communications became a critical tool in monitoring groups like Jemaah Islamiyah (Fahmi Nooryadi et al., 2025).

2. Limitations of Traditional Intelligence Methods

   Despite their importance, both HUMINT and SIGINT have increasingly shown limitations in addressing modern security challenges. HUMINT, for instance, is time-consuming, often fraught with misinformation, and dependent on the reliability of human sources. These challenges have made it difficult for intelligence agencies to respond swiftly to emerging threats (Dao et al., 2024). Similarly, while SIGINT remains a powerful tool, it faces significant obstacles due to the widespread use of encrypted communication technologies. Today, adversaries use secure digital communication platforms, including the dark web and encrypted apps, which traditional SIGINT methods struggle to intercept (Fahmi Nooryadi et al., 2025). Additionally, the explosion of big data has overwhelmed traditional methods, making it difficult for analysts to keep pace with rapidly evolving threats (Macêdo et al., 2023).

   As the digital age progressed, intelligence agencies in Indonesia recognized the need to integrate emerging technologies such as AI-driven analytics and social media monitoring to complement traditional methods. These digital tools provide intelligence agencies with the ability to collect and analyze vast amounts of data more efficiently, helping them respond faster and more effectively to new security threats.

Introduction of Digital Technology in Intelligence

The 21st century ushered in a new era for intelligence operations in Indonesia, as the rise of digital technologies began to transform how intelligence was gathered and processed. This section examines the early adoption of digital tools, such as surveillance systems and data analytics, and how these technologies have shaped both the national and global intelligence landscapes.

1. Early Adoption of Technology in Indonesia's Intelligence Practices

   In the late 20th and early 21st centuries, Indonesia began integrating digital technologies into its intelligence operations. Initially, these technologies were used to enhance existing intelligence methods, focusing on improving surveillance and data management systems. The rapid expansion of the internet in the 1990s pushed Indonesia's intelligence community to adopt new tools that could secure critical national infrastructure and monitor emerging threats, particularly online extremism and terrorism (Macêdo et al., 2023).

   The National Intelligence Agency (BIN) was one of the first to experiment with digital tools, including database management systems, for organizing intelligence data. This shift was driven by the growing importance of cybersecurity and the realization that traditional intelligence methods were no longer sufficient to address the complexities of the digital age. Early investments in securing telecommunication infrastructure, monitoring internet traffic, and developing cybersecurity frameworks marked Indonesia's first steps in modernizing its intelligence infrastructure (Dao et al., 2024).

2. Examples of Initial Integrations: Surveillance Systems and Data Analytics

   A key area where digital technologies were integrated was surveillance. In the early stages, Indonesia implemented closed-circuit television (CCTV) systems and geospatial intelligence (GEOINT) to monitor public spaces, including government buildings, airports, and border areas. These systems are instrumental in preventing terrorism and monitoring security threats. As Indonesia faced growing maritime threats, these surveillance technologies were also applied to monitor sea lanes, which are crucial for national security and economic stability (Kusmantoro et al., 2024).

   Data analytics also play a significant role in Indonesia's initial integration of digital tools. Intelligence agencies have begun utilizing data mining techniques to analyze online communications, including social media platforms, and to identify early indicators of radicalization or terrorist activity. The ability to analyze large volumes of unstructured data is a significant advancement in intelligence gathering, allowing for quicker identification of threats and a more proactive approach to counterterrorism (Fahmi Nooryadi et al., 2025).

3. Global Technological Evolution and Its Influence on Indonesia's Intelligence Landscape

   Globally, technological advancements have significantly reshaped the intelligence landscape. Following the Cold War and 9/11 attacks, intelligence agencies worldwide, particularly in the United States, embraced digital technologies such as big data analytics, surveillance systems, and cyber intelligence to combat terrorism (Surjatmodjo et al., 2024). The success of these technologies in countering global terrorism has set a model for other nations, including Indonesia, to modernize their intelligence frameworks.

   For Indonesia, the rise of new technologies, such as artificial intelligence (AI) and real-time data analytics, has become essential in managing increasingly complex threats from terrorism, cybercrime, and geopolitical instability. As digital technologies continue to evolve, Indonesia seeks to align its intelligence capabilities with these global trends. This includes the adoption of AI for analyzing vast datasets and the integration of cloud-based systems for more efficient data sharing and collaboration with international partners (Yusriadi et al., 2023).

Key Shifts in Security Threats and Intelligence Needs

As Indonesia's intelligence practices have evolved, the nature of security threats has also changed dramatically. While domestic insurgencies and separatism were once the primary concerns, new challenges,

such as cyber threats, terrorism, and online extremism, have emerged as the dominant security issues of the 21st century.

1. Emergence of Cyber Threats, Terrorism, and Online Extremism

   Internet and digital technologies have transformed global security dynamics. In Indonesia, terrorist groups such as Jemaah Islamiyah have increasingly turned to the internet for propaganda, recruitment, and attack coordination. Social media platforms such as Facebook and Twitter have become critical tools for these groups, allowing them to reach global audiences with minimal physical presence. This shift has made it much harder for traditional intelligence methods to track and counter these groups, as they operate in decentralized, often anonymous, environments (Agarwal & Sureka, 2015).

   The rise of lone-actor terrorism, in which individuals carry out attacks inspired by extremist content online, has further complicated intelligence efforts. These attacks are less predictable and harder to prevent because they do not involve coordinated group efforts (Binder & Kenyon, 2022). Cyberattacks also pose a growing threat to national security, with critical infrastructure becoming increasingly vulnerable to hacking and ransomware attacks. In Indonesia, vulnerabilities in areas such as telecommunications, power grids, and financial systems have made them prime targets for cybercriminals and state-sponsored cyber operations (Naidoo & Jacobs, 2023).

2. Technological Solutions for New Intelligence Demands

   The emergence of cyber threats, terrorism, and online extremism has prompted the adoption of new intelligence technologies. Traditional methods, such as HUMINT and SIGINT, while still valuable, are no longer sufficient to address the scale and complexity of modern threats. AI, big data analytics, and social media monitoring have become indispensable tools for modern intelligence operations. AI systems, for instance, can identify patterns in online behavior that may indicate radicalization, allowing intelligence agencies to take action before a threat materializes (Tahat et al., 2024).

   Big data analytics allows intelligence agencies to sift through vast amounts of digital data and extract actionable intelligence. By analyzing internet traffic, social media content, and financial transactions, agencies can track potential threats and identify individuals or networks that may be planning attacks (Ghawa et al., 2023). Cyber threat intelligence, powered by AI and machine learning, enables real-time detection of vulnerabilities and attacks, helping agencies respond proactively rather than reactively (Naidoo & Jacobs, 2023).

3. The Rising Importance of Digital Tools: AI, Big Data, and Social Media Monitoring

   As the threat landscape continues to evolve, digital tools have become increasingly important in intelligence operations. AI, big data analytics, and social media monitoring enable agencies to detect and mitigate threats in real time. The ability to analyze vast amounts of unstructured data, identify radicalization trends, and predict potential incidents has become essential for gathering modern intelligence (Tahat et al., 2024).

   In particular, social media monitoring has become a key tool for identifying signs of online extremism. By using AI to analyze patterns in social media activity, intelligence agencies can track the activities of known extremists, identify emerging threats, and take preventive measures before violence occurs. Predictive analytics also plays a vital role in forecasting potential security incidents based on historical data, helping agencies respond more swiftly and effectively to emerging threats (Naidoo & Jacobs, 2023)

3.2. Overview of Digital Technologies and Their Relevance to Intelligence

Artificial Intelligence (AI) and Machine Learning in Intelligence

1. Basic Concepts of AI and Machine Learning

   Artificial Intelligence (AI) involves the simulation of human cognitive functions in machines, enabling them to perform tasks such as learning, reasoning, and problem-solving (Xu et al., 2021). Machine Learning (ML), a subset of AI, refers to the development of algorithms that enable computers to learn from data, improving their performance over time without explicit

programming. This distinction positions AI as a broader concept that encompasses various computational models, whereas ML specifically focuses on systems that learn from data and improve autonomously (Carissa & Turnip, 2023).

In the context of intelligence, AI systems process vast amounts of data using complex algorithms, identify patterns, make predictions, and support the decision-making processes. AI's ability to learn from large datasets allows it to support intelligence operations in real time, offering insights that are crucial for national security and public safety.

2. Applications of AI in Data Analysis, Surveillance, and Predictive Intelligence

AI and ML are pivotal in modern intelligence operations, particularly in data analysis, surveillance, and predictive intelligence. Intelligence agencies utilize AI to process vast amounts of structured and unstructured data and extract valuable insights to enhance operational efficiency. AI's role in threat detection is significant, aiding in the identification of potential terrorist activities, cyber-attacks, and other criminal behaviors before they escalate (Sarzaeim et al., 2023).

AI-driven surveillance systems, such as facial recognition, motion detection, and behavioral analysis, enable real-time monitoring and early identification of threats. These technologies enhance public safety by detecting suspicious activities in public spaces and critical infrastructure sites. For example, AI-based facial recognition systems can scan crowds to identify individuals of interest (Furkan & Susila, 2024). Additionally, predictive intelligence uses historical data patterns to forecast future risks, such as crime hotspots or terrorist threats, allowing law enforcement agencies to deploy resources more effectively (Furkan & Susila, 2024).

3. Case Studies of AI Integration in Intelligence Agencies Worldwide (With a Focus on Indonesia)

Global intelligence agencies have incorporated AI and ML technologies to streamline their operations and improve threat detection. For example, the United States uses AI extensively in surveillance, including facial recognition programs at airports, whereas the United Kingdom applies AI in analyzing large datasets to predict and prevent terrorist activities (Sarzaeim et al., 2023). AI's adoption by law enforcement agencies globally has led to enhanced crime detection, improved investigative processes, and more effective criminal behavior prediction (Carissa & Turnip, 2023).

In Indonesia, AI adoption in intelligence agencies is still in its nascent stages but shows significant promise. Efforts are underway to integrate AI into predictive policing and to analyze data from social media and public databases to identify early signs of criminal activity. Additionally, AI is being explored in disaster management, such as flood forecasting, which is particularly vital for disaster-prone countries like Indonesia (Riza et al., 2020). A notable example is the use of machine learning models to predict crime patterns in urban areas, particularly in cities such as Jakarta. However, challenges such as infrastructure gaps, privacy concerns, and regulatory issues hinder the broader implementation of AI technologies (Yusriadi et al., 2023).

Despite these challenges, the potential of AI in intelligence is evident as Indonesia continues to invest in technological infrastructure and international collaborations aimed at advancing AI research and applications across multiple sectors (Fauzi, 2024).

Big Data and Data Analytics in Intelligence

1. Importance of Big Data in Modern Intelligence Operations

Big data plays a pivotal role in modern intelligence operations, enabling agencies to process and analyze vast datasets from diverse sources in real time. The surge in digital data from social media, sensors, and public databases has made traditional data analysis methods insufficient for managing and interpreting complex intelligence data (Adekunle Oyeyemi Adenyi et al., 2024). Big data analytics helps uncover hidden patterns, predict future events, and detect emerging threats, thereby enhancing national security and operational efficiency (Jamarani et al., 2024).

For example, big data can be used to analyze communication networks to detect anomalies that may indicate security risks, including terrorist activities or cyber-attacks. Predictive models

leveraging big data allow intelligence agencies to anticipate risks and ensure a proactive approach to security (Jamarani et al., 2024).

2. Techniques Used for Processing and Analyzing Large Datasets

   To handle large datasets, intelligence agencies use several advanced techniques, including predictive analytics, sentiment analysis, and data mining.

   1) Predictive Analytics: Predictive analytics applies statistical models and machine learning to forecast future trends and behaviors based on historical data. It is crucial in threat detection, forecasting potential terrorist attacks, criminal activities, and cybersecurity breaches (Mujawar & Kulkarni, 2017).
   2) Sentiment Analysis: Sentiment analysis involves analyzing text data, such as social media posts, to gauge public opinion and detect potential social unrest or threats. This technique is particularly valuable for monitoring public sentiment and responding to emerging security issues (Ren, 2025).
   3) Data Mining: Data mining techniques help identify patterns, correlations, and anomalies in large datasets. These tools can uncover hidden connections, such as identifying terrorist cells or covert networks, which would otherwise remain undetected (Chen et al., 2022).

3. The Role of Data Mining and Analytics Tools in Identifying Patterns and Threats

   Data mining and analytics tools are essential in modern intelligence operations for identifying patterns and threats. By analyzing vast datasets, these tools can detect unusual patterns or behaviors that indicate emerging risks. For example, predictive models can identify potential cyber-attacks or terrorist activities based on past behavioral patterns. On the other hand, sentiment analysis helps monitor public sentiment, allowing agencies to take preemptive measures during periods of civil unrest or social turmoil (Rubeis, 2022).

Social Media and Cyber Intelligence

1. The Impact of Social Media in Contemporary Intelligence Gathering

   Social media platforms such as Twitter, Facebook, and Instagram have revolutionized intelligence gathering by providing real-time access to unstructured data. Intelligence agencies now leverage these platforms to monitor public sentiment, track extremist groups, and detect early signs of radicalization (Agarwal & Sureka, 2015). Social media serves as an unfiltered window into the public's opinions, social movements, and emerging security threats, allowing intelligence agencies to identify potential risks before they escalate into crises (Tahat et al., 2024).

2. Case Studies of How Social Media is Used to Detect Terrorism, Extremism, and Public Sentiment

   The role of social media in detecting terrorism and extremism is well documented. In Indonesia, for example, terrorist organizations use social media to spread propaganda, recruit followers, and coordinate attacks. Researchers have developed machine learning tools to identify extremist content and online radicalization through social media analysis (Huda et al., 2021). Social media platforms also play a key role in gauging public sentiment, which is essential during civil unrest or terrorist-related events (Md Suhaimin et al., 2023).

3. Challenges in Monitoring and Analyzing Unstructured Data from Social Media Platforms

   Despite its potential, the analysis of unstructured social media data presents several challenges. The sheer volume and complexity of social media content, including slang, abbreviations, and varied languages, make it difficult to extract meaningful insights. Additionally, the continuous evolution of online radicalization tactics requires intelligence agencies to develop adaptive, real-time monitoring systems to track emerging threats (Sundaram et al., 2023).

   Ethical and privacy concerns also complicate the use of social media for intelligence. Balancing national security with privacy rights is a significant challenge, as unrestricted surveillance may infringe upon individual freedoms. Furthermore, algorithmic bias in social media monitoring systems can lead to discrimination, particularly if AI models are trained on biased data (Gaikwad et al., 2021).

The Role of Digital Surveillance Technologies

1. Types of Digital Surveillance Technologies

   Digital surveillance technologies, including facial recognition, drones, and network monitoring systems, play a crucial role in enhancing intelligence operations and national security.

   1) Facial Recognition: Facial recognition technology uses biometric data to match individuals' faces against a database, aiding law enforcement in tracking suspects in public spaces (Gohari et al., 2022).
   2) Drones: Drones provide real-time aerial surveillance and are particularly useful for monitoring large areas or conducting reconnaissance in remote or dangerous locations (Kumar et al., 2025).
   3) Network Monitoring: Network monitoring tools allow intelligence agencies to track digital communications, detect anomalies, and prevent cyber-attacks or terrorist communications (Agarwal & Sureka, 2015).

2. Ethical Concerns and Privacy Issues

   Although digital surveillance technologies offer significant advantages, they also raise ethical and privacy concerns. These include the potential invasion of privacy, data security risks, and the misuse of surveillance capabilities. The deployment of technologies such as facial recognition and drones has sparked debates about the balance between national security and individual freedoms (Tahat et al., 2024).

3. Adoption of Digital Surveillance Technologies by Indonesian Intelligence Agencies

   In Indonesia, intelligence agencies have increasingly adopted digital surveillance technologies to enhance national security and combat terrorism. The National Intelligence Agency (BIN) and Counter-Terrorism Unit (Densus 88) have incorporated drones, facial recognition, and network monitoring to detect potential threats (Furkan & Susila, 2024). However, the adoption of these technologies has been met with concerns about privacy, ethics, and the need for regulations to ensure responsible use (Mariyam, 2024).

3.3. Key Challenges in Integrating Digital Technologies in Indonesian Intelligence

Infrastructure and Technological Gaps

1. Overview of the Current State of Digital Infrastructure in Indonesia's Intelligence Agencies

   The rapid evolution of digital technologies has significantly affected Indonesia's intelligence agencies, presenting both opportunities and challenges. As the country seeks to modernize its national security apparatus, the digital infrastructure required to support sophisticated technologies such as Artificial Intelligence (AI), big data analytics, and cybersecurity tools remains underdeveloped. While there has been gradual progress in integrating digital tools within intelligence operations, many obstacles persist, especially in rural and remote regions (Wulandari et al., 2025).

   Indonesia's intelligence agencies, including the National Intelligence Agency (BIN), Indonesian National Police (POLRI), and TNI Cyberforce, have made initial efforts to adopt advanced technologies. However, existing infrastructure is often insufficient, with gaps in computing power, data storage, and secure communication systems. The country's digital infrastructure suffers from a significant digital divide, further exacerbated by slow regulatory reforms that have hindered the full integration of these technologies into intelligence operations (Samingan et al., 2024). As a result, Indonesia faces challenges in maintaining scalable systems capable of processing and analyzing vast datasets in real time, which is critical for surveillance, counter-terrorism, and cyber defense efforts.

2. Challenges Related to the Lack of Sufficient Hardware, Software, and Secure Communication Channels

   Indonesia's intelligence agencies face several infrastructure deficiencies that impede the effective integration of digital technologies into intelligence operations. These deficiencies include

limitations in hardware, software, and secure communication channels, all of which are vital for ensuring the success of modern intelligence practices.

1) Hardware Limitations: The lack of high-performance hardware remains a key bottleneck for Indonesia's intelligence agencies. Many agencies are still reliant on outdated systems that struggle to process large datasets generated from surveillance tools, such as drones, satellite imagery, and smart sensors. Modern intelligence operations require an advanced computing infrastructure capable of handling the massive volumes of data generated by these technologies. However, building and maintaining such infrastructure remains a challenge (Yusriadi et al., 2023). In addition, many government agencies face a lack of redundancy and resilience in their hardware systems, which is critical for maintaining national security in the face of potential cyberattacks.
2) Software and Analytical Tools: The software solutions available for data analysis within Indonesia's intelligence agencies are often inadequate. These agencies require software capable of handling a wide variety of unstructured data sources, such as social media, video feeds, and audio recordings. However, the lack of advanced machine learning (ML) and natural language processing (NLP) tools in Indonesia's intelligence community hinders the effective processing of these data (Samingan et al., 2024). Furthermore, reliance on legacy systems and siloed software further complicates interagency cooperation, slowing down analysis and response times in critical situations.
3) Secure Communication Channels: A major concern in Indonesia's intelligence sector is the lack of secure and reliable communication channels for transmitting sensitive data. Despite improvements in cybersecurity, a country's intelligence agencies remain vulnerable to cyberattacks, which can compromise the confidentiality of national security operations. Secure communication technologies, such as encryption, are critical for safeguarding intelligence information. However, Indonesia's intelligence agencies have struggled to develop robust communication systems that can withstand sophisticated cyber threats (Ishak, 2023). This issue is particularly concerning, as intelligence agencies rely on digital channels for sharing sensitive data, increasing the risk of espionage or data breaches.

3. Cybersecurity and Data Protection

Although Indonesia's cybersecurity framework is evolving, it faces numerous challenges. Data security and protection, especially within the intelligence sector, have become pressing concerns owing to the growing threat landscape. Cyberattacks, including ransomware and data breaches, can compromise critical intelligence data. Additionally, Indonesia faces ongoing challenges in enforcing data protection laws, such as the Personal Data Protection Law (PDP), particularly within the intelligence and defense sectors (Wulandari et al., 2025). To safeguard national security, the country needs to develop a comprehensive infrastructure for secure data storage and processing while improving its defense against increasingly sophisticated cyber-attacks.

Data Security and Cybersecurity Issues

1. Risks Associated with Digital Data Storage and Transfer

With increasing reliance on digital technologies, data security has become a critical issue for Indonesia's intelligence agencies. Digital data storage and transfer carry significant risks, particularly regarding the confidentiality, integrity, and availability of sensitive information. As digital technologies advance, the risks associated with cyberattacks and data breaches escalate, with potentially devastating consequences for national security.

1) Data Breaches: Data breaches remain one of the most prominent risks faced by Indonesia's intelligence agencies. The increasing volume of stored data, including classified intelligence and personal information, increases the risk of unauthorized access. These breaches may arise from external cyberattacks, insider threats, or poor access to control measures. Cyberattacks, such as ransomware, spear-phishing, and espionage, are commonly used to steal sensitive data, leading to significant security risks (Wulandari et al., 2025).
2) Data Integrity and Loss: Data loss or corruption is another significant risk in Indonesia's intelligence sector. Cyberattacks such as ransomware can compromise the integrity of

critical intelligence data, potentially leading to the loss of vital information. Inadequate backup and recovery protocols increase the likelihood of permanent data loss, which can severely disrupt national security operations (Sun, 2024).

3) Secure Data Transfer: Data transfer, especially across networks, poses a substantial risk in Indonesia's intelligence operations. Unsecured communication channels, particularly those relying on standard Internet Protocol (IP) networks, expose sensitive data to cyberattacks, such as man-in-the-middle (MitM) attacks, where malicious actors can intercept and manipulate data in transit. To mitigate these risks, intelligence agencies must implement advanced encryption techniques and secure transmission protocols such as SSL/TLS and multifactor authentication (Permana, 2021).

2. Case Studies of Cybersecurity Breaches and Lessons Learned

Several high-profile cybersecurity breaches in Indonesia have highlighted the vulnerabilities of its digital infrastructure, particularly in sectors related to national security.

1) Data Breaches in Government Systems: A significant breach involved the National Identity System (NIK), where millions of personal identification numbers were exposed, leading to concerns about identity theft and fraud. This incident revealed gaps in data governance and cybersecurity infrastructure, undermining public trust in government institutions (Sari et al., 2024).
2) Cyberattacks on Critical Infrastructure: Indonesia's TNI Cyberforce has responded to several targeted cyberattacks on critical military and governmental IT infrastructure. These attacks, which are attributed to foreign actors, seek to manipulate public opinion or gather intelligence. Indonesia's response focuses on strengthening cybersecurity measures including improved data encryption and enhanced monitoring systems (Wulandari et al., 2025).
3) Ransomware Attacks: Ransomware attacks targeting critical public services and businesses have caused significant disruptions in Indonesia. These attacks encrypt organizational data and demand a ransom for their release, highlighting the need for improved cyber hygiene, vulnerability assessments, and employee training (Sun, 2024).

3. Strategies for Strengthening Digital Security in Intelligence Operations

To improve data security, Indonesia's intelligence agencies must adopt a multilayered cybersecurity strategy.

1) Enhanced Cybersecurity Frameworks: Indonesia must evolve its cybersecurity strategy to prevent, identify, and remedy cyber threats. A national cybersecurity policy that strengthens frameworks across government agencies with an emphasis on data protection, risk management, and incident response is crucial (Permana, 2021).
2) Encryption and Secure Communication: The adoption of end-to-end encryption and secure communication protocols is vital for safeguarding intelligence data during transfer. Indonesia's intelligence agencies should prioritize the development of secure channels for sharing classified information (Sun, 2024).
3) AI-Driven Cybersecurity: AI offers promising solutions for real-time threat detection and response. Integrating AI-driven tools into cybersecurity frameworks can help Indonesia's intelligence agencies identify anomalies and swiftly mitigate risks (Sari et al., 2024).
4) Training and Public Awareness: Continuous training and public awareness campaigns focused on cybersecurity best practices are critical for enhancing security. Educating employees and citizens about the importance of safe data handling and identifying cyber threats can significantly reduce vulnerability (Tatara et al., 2023).

3.4. Opportunities for Enhancing Intelligence through Digital Technology

Collaboration with the Private Sector and Technology Firms

1. Opportunities for Public-Private Partnerships to Enhance Digital Capabilities

The integration of digital technologies into Indonesia's intelligence and security sectors presents a significant opportunity for collaboration with private sector firms, particularly those specializing in technology. Public-private partnerships (PPPs) have become a vital mechanism for

enhancing the digital capabilities of government agencies, enabling the public sector to access state-of-the-art technologies and expertise that might otherwise be out of reach. This is especially important in areas such as artificial intelligence (AI), machine learning, big data analytics, and cybersecurity.

Public-private collaborations allow for the sharing of risks and responsibilities, creating an environment where both parties can leverage their strengths. For example, global tech giants such as Google, Microsoft, and IBM have partnered with governments worldwide to implement AI solutions, cloud computing, and big data analytics for national security and public service improvements (Gupta et al., 2025). Indonesia's intelligence agencies could greatly benefit from similar collaborations, allowing them to harness advanced data analytics and AI-powered predictive models, enhancing intelligence operations, and improving response times to security threats.

In addition to technology sharing, public-private partnerships can also help bridge the digital divide by ensuring that high-quality digital services are available to underserved regions of the country. By collaborating with technology firms, Indonesia can build secure, scalable infrastructure capable of processing and analyzing large datasets generated from intelligence operations and surveillance (Fauziddin et al., 2025). These collaborations could help modernize Indonesia's intelligence infrastructure, ultimately leading to better threat detection, cyber defence, and predictive intelligence capabilities.

2. Example Collaborations Globally and in Indonesia

Several global collaborations between the private sector and government agencies illustrate the potential benefits of public-private partnerships in enhancing intelligence capabilities. One prominent example is the partnership between Microsoft and the U.S.. Department of Defense, where AI-driven defense technologies have been developed for use in predictive analytics, autonomous systems, and cybersecurity solutions (Gupta et al., 2025). Similarly, in Singapore, the government has partnered with tech companies, such as Google and Amazon Web Services, to integrate AI into urban planning, healthcare, and national security applications, enhancing the country's ability to respond to emerging threats and improving public services (Furkan & Susila, 2024).

In Indonesia, there have also been notable examples of public-private partnerships aimed at enhancing intelligence capabilities. The Indonesian National Police (POLRI) has collaborated with technology firms to develop AI-driven tools for crime prevention, data analysis, and cybersecurity, thereby improving the accuracy and speed of criminal investigations (Yusriadi et al., 2023). Furthermore, the Indonesian National Intelligence Agency (BIN) has worked with local tech companies to implement AI-based surveillance systems for national security. These collaborations aim to develop real-time data collection, analysis, and threat detection systems that are crucial for responding to emerging security risks.

One notable initiative in Indonesia is the Smart Government Project, which aims to leverage AI to improve public services including law enforcement and healthcare. Through partnerships with the private sector, the Indonesian government is enhancing its technological capabilities and infrastructure to provide more efficient and effective services to citizens (Aryanto et al., 2023).

3. Challenges and Future Directions

While public-private partnerships offer significant opportunities, they also come with challenges. One of the primary concerns is the power imbalance between large tech firms and government entities. As Gupta et al. (2025) point out, the dominance of big-tech firms in such collaborations may lead to issues around data control, ethical concerns, and dependency on private companies. Indonesia must ensure that these partnerships remain equitable with clear regulations that protect the country's national interests and the rights of its citizens.

Data privacy and transparency are also critical concerns in public-private collaborations. The integration of AI, big data, and cloud computing into intelligence operations raises significant ethical and privacy questions, particularly regarding the collection, storage, and use of personal

data. Indonesia must ensure that these partnerships comply with the Personal Data Protection Law (PDP Law) and other relevant regulations to maintain public trust (Fauziddin et al., 2025).

To maximize the benefits of these partnerships, Indonesia must continue to develop strong frameworks for collaboration, focusing on capacity building, skill development, and joint ventures with international technology firms. These efforts will not only foster innovation but also enable Indonesia to keep pace with global advancements in AI and cybersecurity, ultimately enhancing national security and improving the country's digital infrastructure.

Strengthening Intelligence Sharing with International Agencies

1. How Global Intelligence Networks Integrate Digital Technologies

   International intelligence networks, such as Five Eyes and INTERPOL, play a vital role in fostering collaboration and intelligence sharing, particularly through digital technologies. These networks are increasingly integrating advanced technologies to enhance their capacity to address global security threats including terrorism, cybercrime, and transnational criminal activities.

   The Five Eyes network, comprising the United States, the United Kingdom, Canada, Australia, and New Zealand, uses cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics to improve the speed and accuracy of information sharing among member nations. By leveraging these technologies, the Five Eyes network enables real-time analysis of massive data volumes, enhancing threat detection, and improving intelligence sharing (Papageorgiou & Leoni, 2025).

   Similarly, INTERPOL has adopted digital technologies to strengthen cross-border law enforcement collaboration. INTERPOL's I-24/7 network allows member countries to exchange data securely, including criminal records, intelligence reports, and biometric data. Recently, AI-driven data analytics and biometric identification technologies have been integrated into INTERPOL's operations to improve crime detection and tracking of criminal networks (Furkan & Susila, 2024). These developments have enabled INTERPOL to enhance its support for international counterterrorism efforts and fight against organized crime.

   The integration of digital technologies into global intelligence networks also facilitates the development of data-sharing platforms, where member countries can exchange real-time information about emerging threats. Using automated alerts and predictive analysis, these platforms enhance the ability of member nations to respond promptly to potential security risks. Digital technologies are transforming these networks and enhancing their ability to track, monitor, and share intelligence on a global scale.

2. Benefits and Challenges of Enhancing Indonesia's Intelligence Sharing via Digital Platforms

   Strengthening Indonesia's intelligence-sharing capabilities through digital platforms offers numerous benefits and challenges. Key advantages include enhanced threat detection, global expertise, and improved diplomatic relations.

   1) Enhanced Security and Threat Detection: By participating in global intelligence-sharing platforms, Indonesia can enhance its ability to detect and address cybersecurity threats, terrorism, and organized crime. The integration of AI, machine learning, and big data analytics will significantly improve Indonesia's predictive intelligence, helping authorities identify potential threats before they escalate (Fauziddin et al., 2025).
   2) Access to Global Expertise and Resources: Collaboration with international intelligence networks provides Indonesia with access to a wealth of expertise, technology, and resources. By working with global partners, Indonesia can improve its intelligence operations through access to cutting-edge technologies and specialized training, particularly in the fields of AI and cybersecurity (Wulandari et al., 2025).
   3) Strengthened Diplomatic and Security Relations: By enhancing intelligence sharing, Indonesia can strengthen its diplomatic and security relations with global partners. This cooperation can lead to better coordination in combating international threats, such as terrorism and cybercrime, which often transcend national borders (Nur et al., 2024).

However, several challenges must be addressed, including:

1) Legal and Regulatory Barriers: Indonesia must navigate complex legal and regulatory frameworks surrounding data sharing and privacy rights. The Personal Data Protection Law (PDP) and other regulations must be aligned with global standards to facilitate smooth and ethical intelligence sharing (Ishak, 2023).
2) Data Security and Privacy Concerns: Sharing intelligence data across borders raises significant data security and privacy concerns. Indonesia must ensure that sensitive national data are protected from misuse and cyberattacks. Robust encryption and secure communication systems are essential for protecting national security and maintaining public trust (Yusriadi et al., 2023).
3) Interoperability and Technological Gaps: Technological gaps remain a challenge for Indonesia's intelligence agencies, particularly in terms of interoperability with international platforms. Upgrading digital infrastructure and investing in new technologies are necessary to ensure seamless integration with global intelligence networks (Ishak, 2023).
4) Cultural and Organizational Challenges: Trust and communication between international agencies can be hindered by national interests and differing operational approaches. Indonesia must foster a culture of cooperation and trust with international partners while ensuring that its national interests are safeguarded (Nur et al., 2024).

4. Conclusion

Indonesia's intelligence operations have evolved from traditional HUMINT and SIGINT methods to increasingly rely on digital technologies such as AI, big data analytics, and digital surveillance. This shift reflects the need to address modern threats like cybercrime, terrorism, and online extremism. Digital tools enable faster data processing, real-time threat detection, and more proactive security responses. However, this transformation faces major challenges, including limited digital infrastructure, cybersecurity vulnerabilities, regulatory barriers, and a shortage of skilled personnel. Data breaches and cyberattacks highlight the need for stronger cybersecurity frameworks and secure communication systems. To overcome these obstacles, Indonesia must invest in infrastructure, enhance cybersecurity, and develop human capital. Public-private partnerships and international intelligence cooperation offer significant opportunities to bridge technological gaps and improve intelligence capabilities. By strengthening collaboration, infrastructure, and ethical governance, Indonesia can modernize its intelligence system and better respond to evolving national and global security threats.

References

Adekunle Oyeyemi Adenyi, Chioma Anthonia Okolo, Tolulope Olorunsogo, & Oloruntoba Babawarun. (2024). Leveraging big data and analytics for enhanced public health decision-making: A global review. *GSC Advanced Research and Reviews*, *18*(2), 450–456. https://doi.org/10.30574/gscarr.2024.18.2.0078

Agarwal, S., & Sureka, A. (2015). *Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Threats*. https://doi.org/10.48550/arXiv.1511.06858

Al-Suqri, M. N., & Gillani, M. (2022). A Comparative Analysis of Information and Artificial Intelligence Toward National Security. *IEEE Access*, *10*, 64420–64434. https://doi.org/10.1109/ACCESS.2022.3183642

Aryanto, E., Mabruk, H., & Narendroputro, W. (2023). Artificial Intelligence Implementation Strategy to Make It Happen Smart Government Indonesia Gold 2045. *International Journal of Science and Society*, *5*(5). https://doi.org/10.54783/ijsoc.v5i5.877

Binder, J. F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.997390

Carissa, J. S., & Turnip, M. (2023). Utilization of Artificial Intelligence in Predicting Crime. *Journal of Computer Networks, Architecture and High Performance Computing*, *6*(1), 108–118. https://doi.org/10.47709/cnahpc.v6i1.3208

Chen, Y., Li, C., & Wang, H. (2022). Big Data and Predictive Analytics for Business Intelligence: A Bibliographic Study (2000–2021). In *Forecasting* (Vol. 4, Issue 4, pp. 767–786). MDPI. https://doi.org/10.3390/forecast4040042

Dao, Y., Ilmu Sosial, J., & Dan Humaniora, P. (2024). Intelijen Maritim Dalam Penanggulangan Destructive fishing Sebagai Ancaman Keamanan Maritim di Wilayah Pesisir dan Pulau-Pulau Kecil. *JURNAL ILMIAH MUQODDIMAH: Jurnal Ilmu Sosial, Politik Dan Humaniora*, *4*. http://jurnal.um-tapsel.ac.id/index.php/muqoddimah

Fahmi Nooryadi, I., Dohamid, A. G., Prihartoro, M., Asimetris, P., Pertahanan Republik Indonesia, U., Bogor, K., & Jawa Barat, P. (2025). Strategi Kolaboratif Kementerian Pertahanan dan BNPT dalam Upaya Penanggulangan Terorisme untuk Memperkuat Keamanan Nasional. *Aurelia: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia*, *4*(1), 1311.

Fauzi, C. (2024). A REVIEW GEOSPATIAL ARTIFICIAL INTELLIGENCE (GEO-AI): IMPLEMENTATION OF MACHINE LEARNING ON URBAN PLANNING. *Jurnal Multidisiplin Indonesia (JMI)*, *3*(1). https://jmi.rivierapublishing.id/index.php/rp

Fauziddin, M., Adha, T. R., Arifiyanti, N., Indriyani, F., Rizki, L. M., Wulandary, V., & Reddy, V. S. V. (2025). The Impact of AI on the Future of Education in Indonesia. *Educative: Jurnal Ilmiah Pendidikan*, *3*(1), 11–16. https://doi.org/10.70437/educative.v3i1.828

Furkan, A., & Susila, M. E. (2024). Artificial Intelligence-Based Crime Prevention Policy in Indonesia. *PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM*, *23*(3).

Gaikwad, M., Ahirrao, S., Phansalkar, S., & Kotecha, K. (2021). Online Extremism Detection: A Systematic Literature Review With Emphasis on Datasets, Classification Techniques, Validation Methods, and Tools. *IEEE Access*, *9*, 48364–48404. https://doi.org/10.1109/ACCESS.2021.3068313

Ghawa, R., Alamri, J., & Alanazi, R. E. (2023). Empowering Cyber Threat Intelligence with AI. *International Journal on Cybernetics & Informatics*, *12*(7), 73–84. https://doi.org/10.5121/ijci.2023.120706

Gohari, A., Ahmad, A. B., Rahim, R. B. A., Supa'at, A. S. M., Razak, S. A., & Gismalla, M. S. M. (2022). Involvement of Surveillance Drones in Smart Cities: A Systematic Review. *IEEE Access*, *10*, 56611–56628. https://doi.org/10.1109/ACCESS.2022.3177904

Gupta, N., Urmetzer, F., & Ansari, S. (2025). Big-tech Strategic Partnerships in Artificial Intelligence. *International Journal of Business and Management*, *20*(3), 57. https://doi.org/10.5539/ijbm.v20n3p57

Huda, A., Runturambi, A., & Syauqillah, M. (2021). Social Media as An Incubator of Youth Terrorism In Indonesia: Hybrid Threat and Warfare. *JURNAL INDO-ISLAMIKA*. https://doi.org/10.15408/jii.v11i1.20362

Ishak, N. (2023). Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges? *Audito Comparative Law Journal*, *4*(2), 108–117.

Jamarani, A., Haddadi, S., Sarvizadeh, R., Haghi Kashani, M., Akbari, M., & Moradi, S. (2024). Big data and predictive analytics: A systematic review of applications. *Artificial Intelligence Review*, *57*(7), 176. https://doi.org/10.1007/s10462-024-10811-5

Kumar, S., Tiwari, A., Ahirwar, Y., Soni, G., & Arafat, M. Y. (2025). The Rise of UAV-Based Smart Surveillance: A Systematic Review of Trends and Technologies. *IEEE Access*, *13*, 181553–181575. https://doi.org/10.1109/ACCESS.2025.3621736

Kusmantoro, Y., Trismadi, T., & Harsono, G. (2024). Pemanfaatan Teknologi Geospatial Intelligence (GEOINT) untuk Peningkatan Keamanan dan Pengelolaan Maritim di Indonesia. *Journal on Education*, *7*(1), 8218–8235. https://doi.org/10.31004/joe.v7i1.7653

Macêdo, A., Peotta, L., & Gomes, F. (2023). A Review of the Intersection Techniques on Humint and Osint. *International Journal on Cybernetics & Informatics*, *12*(1), 1–11. https://doi.org/10.5121/ijci.2023.120105

Mariyam, S. (2024). Conceptualization Of Regulations On The Use Artificial Intelligence Technology In Indonesia. *PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM*, *23*(3).

Md Suhaimin, M. S., Ahmad Hijazi, M. H., Moung, E. G., Nohuddin, P. N. E., Chua, S., & Coenen, F. (2023). Social media sentiment analysis and opinion mining in public security: Taxonomy, trend analysis, issues and future directions. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101776. https://doi.org/https://doi.org/10.1016/j.jksuci.2023.101776

Mujawar, Mr. R. B., & Kulkarni, Dr. D. B. (2017). A Review: Predictive Analytics with Big Data. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, *6*(3), 536–542. https://doi.org/10.17148/ijarcce.2017.63124

Naidoo, R., & Jacobs, C. (2023). *Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework*.

Nur, M., Latif, A., & Waroi, A. (2024). Coordination and Collaboration between Secret Intelligence Agencies and Government Institutions: Challenges, Opportunities, and Dynamics. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS*, *7*(10). https://doi.org/10.47191/ijmra/v7-i10-06

Papageorgiou, M., & Leoni, Z. (2025). The Five Eyes Allies and China: Assessing Threat Perceptions and Power Dynamics. *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-025-09913-w

Permana, A. (2021). INDONESIA'S CYBER DEFENSE STRATEGY IN MITIGATING THE RISK OF CYBER WARFARE THREATS. *Syntax Idea*, *3*(1).

Ren, J. T. (2025). Harnessing public sentiment: A literature review of sentiment analysis in energy research. *Renewable and Sustainable Energy Reviews*, *219*, 115739. https://doi.org/https://doi.org/10.1016/j.rser.2025.115739

Riza, H., Santoso, E. W., Tejakusuma, I. G., Prawiradisastra, F., & Prihartanto, P. (2020). UTILIZATION OF ARTIFICIAL INTELLIGENCE TO IMPROVE FLOOD DISASTER MITIGATION. *Jurnal Sains Dan Teknologi Mitigasi Bencana*, *15*(1), 1–11. https://doi.org/10.29122/jstmb.v15i1.4145

Rubeis, G. (2022). iHealth: The ethics of artificial intelligence and big data in mental healthcare. *Internet Interventions*, *28*, 100518. https://doi.org/https://doi.org/10.1016/j.invent.2022.100518

Samingan, M., Yudho Prakoso, L., & Suwito. (2024). Indonesia's Digital Economic Policy To Increase Economic Resilience. *International Journal Of Humanities Education And Social Sciences (IJHESS)*, *3*(6), 2846–2853. https://ijhess.com/index.php/ijhess/

Sari, J. A., Yuliani, I., Akadira, T., Sunarya, A., & Ating, R. (2024). Data Security and Individual Privacy from the Perspective of Public Administration. *Ilomata International Journal of Social Science*, *5*(3), 818–830. https://doi.org/10.61194/ijss.v5i3.1297

Sarzaeim, P., Mahmoud, Q. H., Azim, A., Bauer, G., & Bowles, I. (2023). A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing. In *Computers* (Vol. 12, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/computers12120255

Srivastava, K. (2023). Artificial Intelligence and National Security: Perspective of the Global South. *International Journal of Law in Changing World*, *2*(2), 77–87. https://doi.org/10.54934/ijlcw.v2i2.63

Sun, X. (2024). The Current Status and Challenges of Cybersecurity Risks. *Internet of Things and Cloud Computing*, *12*(1), 10–16. https://doi.org/10.11648/j.iotcc.20241201.12

Sundaram, A., Subramaniam, H., Hamid, S., & Mohamad Nor, A. (2023). A Systematic Literature Review on Social Media Slang Analytics in Contemporary Discourse. *IEEE Access*, *11*, 132457–132471. https://doi.org/10.1109/ACCESS.2023.3334278

Surjatmodjo, D., Unde, A. A., Cangara, H., & Hasanuddin, Z. (2024). The State Intelligence Agency (BIN) amid the 2024 general election in Indonesia. *Journal of Infrastructure, Policy and Development*, *8*(8). https://doi.org/10.24294/jipd.v8i8.7287

Tahat, K., Habes, M., Mansoori, A., Naqbi, N., Al Ketbi, N., Maysari, I., Tahat, D., & Altawil, A. (2024). Social media algorithms in countering cyber extremism: A systematic review. In *Journal of Infrastructure, Policy and Development* (Vol. 8, Issue 8). EnPress Publisher, LLC. https://doi.org/10.24294/jipd.v8i8.6632

Tatara, B. A., Abdurachman, B., Mustofa, D. L., & Yacobus, D. (2023). The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. *NUANSA Jurnal Penelitian Ilmu Sosial Dan Keagamaan Islam*, *20*(1), 19–37.

Wulandari, R., Priyanto, P., & Hendra, A. (2025). The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats. *Formosa Journal of Applied Sciences*, *4*(2), 615–626. https://doi.org/10.55927/fjas.v4i2.5

Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C. W., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., … Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. In *Innovation* (Vol. 2, Issue 4). Cell Press. https://doi.org/10.1016/j.xinn.2021.100179

Yusriadi, Y., Rusnaedi, Siregar, N. A., Megawati, S., & Sakkir, G. (2023). Implementation of artificial intelligence in Indonesia. *International Journal of Data and Network Science*, *7*(1), 283–294. https://doi.org/10.5267/j.ijdns.2022.10.005