*International Journal Of Humanities Education And Social Sciences* ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 4, Number 5, April 2025, *Page. 2051 – 2061*
Email : editorijhess@gmail.com

# The Impact of Big Data Analytics on Intelligence Gathering and Defence Decision Making

**Tyan Hidayatus Sholihah1[1)], Dangan Waluyo [2)], Jupriyanto[3)], Tri Guntoro Sukarno Putro[4)]**
[1,2,3,4)]Defense Industry, Faculty of Defense Science and Technology , Republic of Indonesia Defense University

*Corresponding Author
Email: tyanedu01@gmail.com

***Abstract***

*The rapid advancement of information technology today has brought great changes. Besides the many benefits obtained, technological developments also require us to be more vigilant and careful in using them because the higher the risks that will be faced, one of which is cybercrime. Big data analysis plays an important role in improving cybersecurity. With its ability to process large amounts of data, identify patterns, and predict threats, big data analytics helps cybersecurity teams detect and respond to attacks more quickly and effectively. Therefore, this paper will discuss the impact of big data analysis on intelligence gathering and decision-making in defence. This study uses descriptive research methods and SWOT methods. The results of the study show that the system thinking model of the impact of big data analysis in the defence sector on intelligence information collection and decision-making in the defence sector can be seen in Figure 1, which consists of loops A and B. The results of the SWOT analysis show that the impact of big data analysis on intelligence information collection and decision-making in the defence sector is divided into some aspects, which are strengths, weaknesses, opportunities, and threats. In terms of strengths, it is increased efficiency and effectiveness, increased situational awareness, and better decision-making. The weaknesses are related to data security, privacy and ethics, and dependence on technology. The opportunities aspect is the potential collaboration between institutions, increasing public awareness, and predictive analysis. Meanwhile, the threat aspect is the threat of cyber, the development of enemy technology, and the proliferation of information*

***Keywords: Big Data Analytics, Decision Making, Defence, Intelligence, Technology***

## INTRODUCTION

Currently, the world has entered the Industrial Revolution 4.0, where the rapid advancement of information technology has brought great changes. This is because technological advances can encourage the development of innovation and increase the progress of modern civilization. The current development of information technology combined with media and computers has given rise to a new tool called the internet. The existence of the internet has given birth to a new paradigm in human life (Ariyaningsih et al., 2023). The various kinds of technology and communication that we currently use cause us to always depend on the advantages and conveniences offered. This will certainly be very useful in human life. On the other hand, technological developments also require us to be more vigilant and careful in using them because the higher the risks that will be faced, one of which is cybercrime.

The term cybercrime was first introduced by (Gibson, 1984) in his novel, Neuromancer. Cybercrime is a crime that utilizes computer technology and internet networks to commit hacking, theft, fraud, and more. Citing data from the National Cyber and Crypto Agency (BSSN), it was recorded that from January to July 2021, there were 741,441,648 cyber threats that had occurred in Indonesia. Various crimes that often occur such as hacking, cracking, cybersquatting, malware (virus/bots/worm), terrorism, and others (Islami, 2017). Various cyber attacks that are rampant occur due to the carelessness and weakness of the technology security system. This can not only attack an individual or organization but also a country, which can be called cyber espionage.

Cyber espionage can be explained by interpreting one word at a time, namely cyber and espionage. Cyber is defined as the "cyber world" where crime takes place, while espionage is an effort to collect information carried out by individuals or countries. Therefore, cyber espionage can be interpreted as the act of seeking information both to targets requested by the government and carried out by unauthorized people by utilizing cyberspace. This type of crime can harm and disrupt the stability of a country's security and defence. This is due to advances in information technology and telecommunications in the digital era that are misused (Mustameer, 2022).

A fundamental aspect of the Industrial Revolution 4.0 is the utilization of big data. Based on (Yang et al., 2019), big data is a complex process to collect, clean, organize, and analyze large data sets to turn raw data into information that can be used in decision-making. The process of processing big data requires sophisticated technology, such as cloud computing, the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, and others. Big data has an important role in helping to improve the effectiveness and efficiency of governance, including detecting crimes, one of which is cybercrime. On the other hand, advanced technology, such as artificial intelligence and machine learning, also makes cyberattacks more sophisticated and difficult to detect.

Big data analytics has changed the landscape of cyber espionage. Therefore, to counter this threat, it is necessary to have a deep understanding of how actors use big data and develop further strategies. Additionally, by understanding the motives and factors that drive cyber espionage, we can take more effective steps to prevent and mitigate cyberattacks. This proves that intelligence information plays a very crucial role in big data analysis to ward off espionage cyber threats. Intelligence provides context, insights, and deep understanding to support decision-making in addressing espionage cyber threats.

There are several previous studies that have a correlation with the current research. (Putro, 2024) shows that in improving intelligence and supporting strategic decisions, the development of efficient and secure big data and AI infrastructure is very important for the TNI (Indonesian National Army). However, there are still several challenges such as integration, data security, and personnel skills, so investment in advanced technology and collaboration is needed to optimize data management and improve Indonesian National Army's response. One of the big data utilization that the Indonesian government has done is in the e-KTP (identity card) project, where all information related to citizens is stored in a large database of the Indonesian government. The weak protection of privacy in cyberspace requires connection and integration between intelligence and government. This is strongly influenced by integrity in the role of intelligence that plays its main tasks, such as investigation, security, or counterintelligence and mobilization (Jayantho et al., 2020). Then, (Sarjito, 2024) emphasized the importance of intelligence to improve situational awareness, make policy decisions, and reduce risk in hybrid warfare situations. With the current situation, the changing challenges of hybrid warfare, leaders are expected to work together to improve their country's intelligence capabilities and make the best use of them. It can therefore be concluded that research in this area has a strategic role to play in improving intelligence capabilities and the effectiveness of defense decision-making. Therefore, this paper will discuss the impact of big data analysis on intelligence gathering and decision-making in defence.

## RESEARCH METHODS

This study uses a descriptive research method of analysis with a qualitative approach and SWOT method. This research was conducted by collecting secondary data obtained through a variety of sources, such as journals, articles, government reports, and others that provide rich

contextual information, to provide a more comprehensive picture of the phenomenon of the problem being studied. Data is collected in the form of words rather than numbers, resulting in a more comprehensive understanding of intelligence gathering and defense decision-making. Modeling and simulation in this research are used to model the impact of big data analysis on intelligence gathering and decision-making in the defense sector by using a system of thought with a Causal Loop Diagram (CLD) model. The CLD model is used to solve complex problems. It is a cause-and-effect modeling model that focuses on the relationships between system components, depicted in a curved line diagram with arrows connecting them.

## RESULT AND DISCUSSION

### Big Data

Big data encompasses various formats, including structured, unstructured, and semi-structured data. In addition, Big data refers to the volume, speed, and diversity of complex data from several sources, including the internet, social media, and sensor devices. Because the data generated is so enormous and diverse, traditional approaches and instruments are ineffective. Therefore, sophisticated technology and algorithms are needed to process and analyze data on such a large scale. Big data has 5 characteristics (5V), which are volume, velocity, variety, veracity, and value (Hermawan, 2024).

Big data can describe the expected knowledge if the process from data collection to processing is carried out appropriately (Niagahoster, 2021). The following are the stages of big data analytics, namely:

1) Data Integration
   Data integration is the process of collecting all data until it becomes big data. In data integration, the main focus is on data collection. All data that has been recorded in the system will be processed in the next step.
2) Data Management
   The data that has been collected is then managed appropriately using certain methods or technologies. In addition, because of the large and complex data, the process of storing or accessing data also uses a large storage space and can be accessed anytime and from anywhere, such as cloud computing.
3) Data Analysis
   All the data that has been stored and grouped according to its type can be analysed for further needs.

### Big Data Analytics

(Guilfoyle et al., 2016) mentioned that big data analysis, commonly called big data analytics, is a set of automated algorithms and processes with specific parameters that humans may control to interpret, characterize, and detect trends in structured and unstructured data. There are several types of big data analysis, namely:

1) Descriptive Analysis
   Descriptive analysis is a common type of analysis to gain an understanding of what is happening in the data. This type of analysis involves mathematical operations in the processing of raw data.
2) Diagnostic Analysis
   Diagnostic analysis is a type of big data analysis aimed at identifying factors or causes that affect a certain event in data. This approach utilizes root cause and causality analysis to understand how an event occurs.
3) Predictive Analytics

Predictive analysis is a form of analysis that focuses on predictions about what may happen in the future based on patterns and trends in historical data. This type of analysis requires specialized techniques, such as machine learning to create predictive models that can aid in decision-making.

4) Prescriptive Analysis
   Prescriptive analysis is a combination of descriptive, diagnostic, and predictive analysis and compares with various conditions faced, which in turn proactively provide the required recommendations.

**Cloud Computing**

Cloud computing is a data processing model that allows access to data and computing resources through the internet (Mutaqin et al., 2023). Computing resources such as servers, applications, data storage, and data services can be accessed over the internet. This makes it easier for users to no longer need to have their own computing resources. Cloud computing is generally divided into the following three types of services:

1) Infrastructure as a Service (IaaS)
   Users rent infrastructure such as servers, storage, and networks to run applications and store data.
2) Platform as a Service (PaaS)
   Users rent application development and testing platforms such as operating systems, web servers, and databases.
3) Software as a Service (SaaS)
   Users rent ready-to-use web-based applications such as email, financial management, and project management.

Cloud computing provides several advantages, such as high accessibility, lower management costs, flexible scale and easy to change as needed, as well as ease of maintenance and management. On the other hand, there are also several risks and challenges that must be considered, including data security issues, dependence on internet networks that are vulnerable to disruptions, the existence of a single vendor, and others. In the military sector, cloud computing can be used to support intelligence data collection and analysis, logistics operations, and enable more effective inter-unit collaboration (Jaatun et al., 2009).

**Artificial Intelligence (AI)**

Artificial intelligence is a technology that allows machines or computers to imitate human intelligence in processing information and making decisions (Mutaqin et al., 2023). This AI technology allows machines or computers to learn from historical data, identify patterns, and then make decisions or predictions based on that data. There are several types of AI technology, including:

1) Machine Learning (ML)
   Machine learning technology enables machines to learn from data and complete tasks without explicit programming.
2) Natural Language Processing (NLP)
   Natural language processing (NLP) is an artificial intelligence technology that enables computers to understand and manipulate human language. It integrates computational linguistics, machine learning, and deep learning to process human language.
3) Computer Vision
   Computer vision is a branch of computer science dedicated to developing digital systems capable of processing, interpreting, and comprehending visual information (such as images and videos) similarly to human perception.
4) Robotics

Robotics is an interdisciplinary field combining science, engineering, and technology. This field involves the design, construction, operation, and usage of machines that replace or accomplish jobs previously performed by human.

The application of AI technology has been widely used in various fields, one of which is defence. The use of technology as an autonomous weapon system, including in drones, provides many benefits to the military. This is because AI-equipped drones can carry out reconnaissance, attack, and logistics missions independently and in groups. However, the use of AI technology also poses several risks and challenges, such as data privacy and cybersecurity. Therefore, appropriate measures are needed to ensure data security and privacy.

**Intelligence Definition**

The term intelligence comes from the English word, intelligence, which means information that is valued for its timeliness and relevance. In the context of national defence, intelligence refers to the collection, analysis, and interpretation of information to provide insights to policymakers regarding threats, opportunities, and risks (Sarjito, 2024). It includes various sources, including human intelligence (HUMIN), signals intelligence (SIGINT), imaginary intelligence (IMINT), open-source intelligence, and cyber intelligence (Sarjito, 2024). Intelligence enables policymakers to make informed decisions, anticipate challenges, and mitigate risks effectively (ODNI, 2019).

Intelligence assists policymakers in understanding geopolitical complexities and making decisions regarding national security and foreign policy by turning data into actionable insights (Sarjito, 2023). These foreign policy decisions and diplomatic engagements support diplomatic efforts to advance national interests and maintain international stability. In addition, intelligence also plays a role in countering transnational threats, such as terrorism, organized crime, weapons proliferation, and others. Therefore, the role of intelligence is crucial in addressing these challenges (Arbani, 2024) .

**Defence Decision-Making**

Decision-making is an act of determining the choice of a number of alternatives available to solve the problem faced based on certain considerations (Satar & Yusri, 2019). The intended choice is the best choice out of a number of options that are possible to implement after considering the risks, costs, effectiveness, efficiency, resources, needs, benefits, and so on. Therefore, decision-making is a conscious and mature action, not by chance.

This decision-making principle is actually built from two strategic elements that are very important to pay attention to. The first is a person who understands the problem or has the authority to make decisions, and the second is the correct method or basis for decision-making. The right person, but the wrong foundation of decision-making, results in big innovative and creative ideas being eliminated by other less innovative ideas. In fact, it may be fatal with considerable risks (Baumgartner, 2010). Likewise, if the basis for decision-making is correct but the decision-makers do not understand the problem, it will result in inappropriate and detrimental decision choices. This applies to various aspects, including defence.

Proper decision-making in the field of defence is at the heart of a strong and secure country. This is because wrong decision-making can be fatal, both in terms of state losses, loss of life, and public trust. In addition, modern defence is now faced with increasingly complex and dynamic threats. In overcoming this, it is necessary to make quick and effective decisions to deal with various scenarios that may occur. Therefore, making the right defence decisions is a key factor in maintaining the security and sovereignty of a country.

**National Defence**

The 2015 White Paper on Indonesia's Defence (Ministry of Defence of the Republic of Indonesia, 2015) states that our country's defence is compiled in a universal defence system formulation to achieve national goals. In essence, universal defence is a defence that involves all

Indonesian citizens according to their roles and functions, in accordance with the mandate of the 1945 Constitution of the Republic of Indonesia. In ensuring national defence, the Indonesian government has formulated a number of agendas, including the study of the development of the strategic environment, the essence of national defence, policies, strategies, and the development of national defence capabilities, the defence industry, international cooperation in the field of defence, national defence, state defence posture, national defence development, and the state defence budget (Ministry of Defence of the Republic of Indonesia, 2015). In that case, of course, it requires a large defence budget. Therefore, in every decision that will be made for the development of national defence, it requires precision, prudence, and relevance of effective outputs and impacts

**System Thinking Analysis the Impact of Big Data Analysis on Intelligence Information Collection and Defence Decision Making**

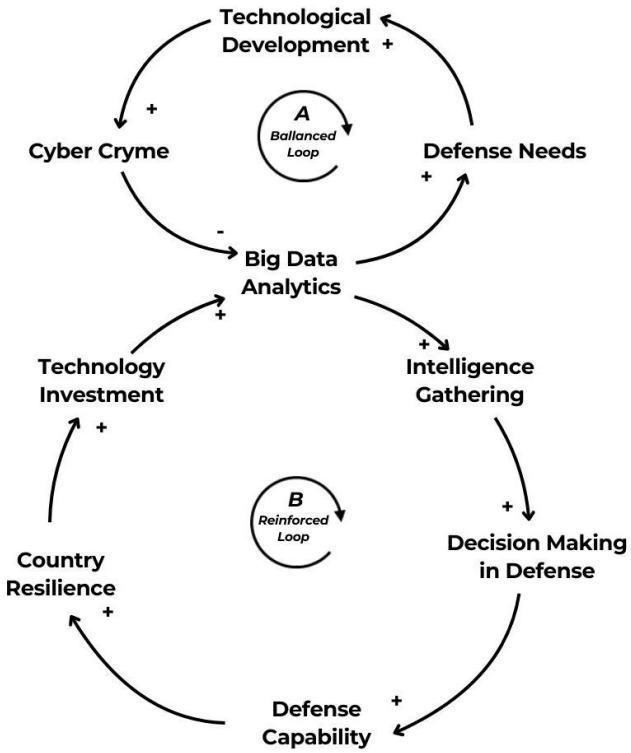


Figure1. System Thinking on the Impact of Big Data Analysis in the Defence Sector
Source: Author's analysis

The figure above is a system thinking about the impact of big data analysis in the field of defence that illustrates the complex relationships between various elements. This system forms a closed loop, which means that improvements in one element will have an impact on other elements, and so on. There are 2 loops, namely loops A and B. In loop A there are 4 elements, namely technological development, cybercrime, big data analytics, and defence need. Meanwhile, in loop B there are 6 elements, consisting of big data analytics, intelligence gathering, decision-making in defence, defence capability, country resilience, and technology investment.

Technological developments are system changes that occur to technology. Cybercrime is a crime committed in cyberspace, while defence needs is everything needed by a country to

maintain national security and sovereignty. Big data analysis is intended to use technology to process and analyse large, complex, and diverse data sets in the defence field. Intelligence gathering is the process of collecting, analysing, and disseminating information about potential enemies, threats, and strategic environments. Furthermore, decision-making is the process of selecting the best course of action based on the information that has been obtained to achieve strategic objectives in the field of defence. Defence capability is the military's ability to protect assets, respond to threats, and achieve strategic objectives. National resilience is the ability of a country to survive threats and maintain stability and security. Then the last is technology investment, a commitment to allocate resources, both financial and non-financial, into the development and application of new technologies.

The following is an explanation of the relationship between the A-loop elements in system thinking as follows:

1) Technological Developments Increase the Potential for Cyber Threats
   The rapid development of technology does bring many benefits, but it also opens up new openings for cybercriminals. This is because as technology becomes more sophisticated, cyberattack methods are also becoming more complex and difficult to detect.
2) Increasing Cyber Threats Require Big Data Analysis
   Big data analysis plays an important role in improving cybersecurity. With its ability to process large amounts of data, identify patterns, and predict threats, big data analytics helps cybersecurity teams to detect and respond to attacks more quickly and effectively.
3) Big Data Analytics Increases Defence Needs
   Today, big data analytics has become a critical component of modern defence. This is because the results of big data analysis allow for more accurate intelligence gathering, more precise threat detection, and better decision-making. Therefore, defence needs will be able to be met optimally.
4) Increasing Defence Needs Drive Technological Development
   The increasing need for defence encourages countries to continue to invest in technology development, especially military technology. This is because the country will continue to strive to improve its defence capabilities in the face of global geopolitical dynamics.

The explanation of the relationship between loop B elements in system thinking above is as follows:

1) Big Data Analytics Improves Intelligence Gathering
   Big data analytics allows the collection of data from a variety of sources, including the internet, social media, censorship, and even from hard-to-access sources. This can expand the scope and depth of intelligence information.
2) Enhanced Intelligence Gathering Helps Decision-Making
   More accurate and comprehensive intelligence information makes it easier for defence policy decision-makers to understand the situation well. So that the decision made is the right decision and can anticipate potential threats that may occur.
3) Informed Decision Making Improves Defence Capabilities
   Appropriate defence decisions in the allocation of strategies, tactics, and resources can improve the effectiveness of military operations and the ability to respond to threats. This can certainly strengthen national defence capabilities.
4) Increased Defence Capabilities Will Increase National Resilience
   Stronger military capabilities can increase the deterrent effect, making the enemy rethink aggression. In addition to reducing the risk of conflict, adequate defence capabilities can also maintain stability and national security.
5) National Resilience Supports Technology Investment

Success in maintaining national security and stability encourages investment in technology and defence resources. One of the reasons is that investors tend to be more interested in investing in countries that have guaranteed political stability and security. In addition, good national resilience is usually accompanied by adequate infrastructure, which is suitable for technological development.

6) Technology Investments Improve Big Data Analytics Capabilities
Investment in technology is indeed the key to improving data analysis capabilities. This is because the more sophisticated the technology used, the deeper and more complex the analysis that can be carried out on big data

**SWOT Analysis the Impact of Big Data Analysis on Intelligence Collection and Defence Decision Making**

SWOT analysis is a method used to identify strengths, weaknesses, opportunities, and threats within an organization or project. Big data analysis in the defence field has great potential to improve intelligence gathering and decision-making capabilities. However, big data analysis also has risks and challenges that need to be considered. Here is a SWOT analysis of the impact of big data analysis on intelligence gathering:

Table 1. SWOT Analysis the Impact of Big Data Analytics on Intelligence Gathering and Defence Decision Making

| No. | Aspects | Analysis |
|---|---|---|
| 1. | **Strengths** | Increased Efficiency and Effectiveness<br>Big data analytics and advanced technologies enable the automation of time-consuming tasks, such as data collection, filtering, and processing. In addition to freeing analysts to focus on more strategic tasks, big data analysis also provides relevant and accurate intelligence information.<br>Situational Awareness Enhancement<br>The insights gained from the results of big data analysis can be used to identify potential threats, monitor the global situation in real-time, and even track the enemy's movements. This provides better situational awareness to decision-makers.<br>Better Decision Making<br>Big data analysis allows the identification of patterns, trends, and anomalies that may not be possible through manual analysis. The information obtained can then be used to make more effective decisions, one of which is in the field of defence. |
| 2. | **Weaknesses** | Data Security<br>Data security is an important issue in data analysis. Data leaks or unauthorized access can compromise intelligence operations and national security. Therefore, strong data security is needed to protect sensitive information.<br>Privacy and Ethics<br>The collection and analysis of large amounts of data sometimes raises questions regarding privacy and ethics. This is because the use of personal information through the collection of big data for intelligence purposes can cause controversy and legal problems.<br>Dependence on Technology |

| | | |
|---|---|---|
| | | As we know, big data analysis in the process relies heavily on sophisticated and complex technology. Therefore, vulnerability to cyberattacks or technological failures can have a serious impact on intelligence gathering capabilities. |
| 3. | **Opportunities** | Inter-Institutional Collaboration<br>Big data analysis facilitates cooperation and collaboration between institutions, both inside and outside the military. This can certainly encourage more optimal information exchange and coordination so that it can increase the efficiency and effectiveness of intelligence collection.<br>Increased Public Awareness<br>The information or insights obtained from big data analysis can be used to increase public awareness of potential threats and dangers faced by countries.<br>Predictive Analytics<br>As previously explained, one form of big data analysis is predictive analytics that can be used to predict potential threats. This is crucial for planning strategies and making more effective defensive decisions. |
| 4. | **Threats** | Cybercrime<br>Attachment to technology makes big data analysis vulnerable to cyberattacks. This is because adversaries can also try to steal data, manipulate information, or disrupt intelligence operations.<br>Enemy Technology Developments<br>The information generated from the analysis of the enemy's big data can certainly also be used to improve their own intelligence capabilities. This can create an imbalance in intelligence capabilities and pose new threats, especially if the enemy has more advanced technology.<br>Information Proliferation<br>Big data analysis faces challenges in managing and analyzing big data, especially due to the ever-increasing volume of data, namely information proliferation. Sometimes the proliferation of information leads to confusion that causes difficulties in identifying relevant information. |

Source: Author's analysis

## CONCLUSION

The system thinking model of the impact of big data analysis in the defence sector on intelligence information collection and decision-making in the defence sector can be seen in Figure 1. In loop A, it can be explained that technological developments increase the potential for cybercrime. In overcoming potential cyber threats, big data analysis is needed to predict potential threats. Then the information obtained from this big data analysis will certainly increase defence needs. The increasing need for defence makes technological developments increase because various sophisticated technologies are needed in action. In loop B, big data analysis allows for the collection of optimal intelligence information, which then affects the right

decision-making. This has an impact on increasing a country's defence capability. Furthermore, this strong defence capability protects the country from various threats, maintaining sovereignty and territorial integrity. This can certainly increase the country's resilience. With good national resilience, it will increase technology investment. This is because investors tend to be more interested in a stable and safe country. Then good technology investment will have an impact on the activities of big data analysts because, in the process, this requires various sophisticated technologies. Besides that, based on the results of the SWOT analysis, the impact of big data analysis on intelligence information collection and decision-making in the defence sector is divided into aspects of strategy, weaknesses, opportunities, and threats. In terms of strategy, the impact of big data analysis on intelligence information collection and decision-making in the defence sector is increased efficiency and effectiveness, increased situational awareness, and better decision-making. The weaknesses are related to data security, privacy and ethics, and dependence on technology. The opportunities aspect is collaboration between institutions, increasing public awareness, and predictive analysis. Meanwhile, the threat aspect is the threat of cyber threats, the development of enemy technology, and the proliferation of information.

## REFERENCES

Arbani. (2024). Pentingnya Badan Intelijen Pertahanan dalam Non-Combat Military Mission: Instrumen Perhatian Khusus untuk Peningkatan Kapasitas dan Kapabilitas Pertahanan. *Jurnal Syntax Admiration, 5, No. 6*(5), p-ISSN.

Ariyaningsih, S., Ari Andrianto, A., Surya Kusuma, A., & Rezi. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum, 1, No. 1*, 1–11.

Baumgartner, J. (2010). *The Way of Innovation Master* (1st ed.). JPB.

Gibson, W. (1984). *Neuromancer*. Ace Books.

Guilfoyle, S., Bergman, S. M., Hartwell, C., & Powers, J. (2016). Social media, big data, and employment decisions: Mo' data, mo' problems? In *Social Media in Employee Selection and Recruitment: Theory, Practice, and Current Challenges* (pp. 127–155). Springer International Publishing. https://doi.org/10.1007/978-3-319-29989-1_7

Hermawan, A. (2024). Mengintip Celah antara Potensi dan Tantangan Big Data pada Layanan Jaminan Sosial Ketenagakerjaan Indonesia. *Jurnal Jamsostek, 2, No. 2*(2). https://doi.org/10.61626/jamsostek

Islami, J. M. (2017). Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. *Jurnal Masyarakat Telematika Dan Informasi*, *8, No. 2*, 137–144.

Jaatun, M. G., Zhao, G., & Rong, C. (2009). *Cloud computing: An overview. In Cloud Computing: First International Conference, Beijing, China, December 2009*. Springer-Verlag Berlin Heidelberg.

Jayantho, S., Runturambi, A. J. S., Ras, A. R., & Widiawan, B. (2020). Pemodelan Sistem Dinamis Stratejik Intelijen Dalam Meminimalisasi Ancaman Spionase dan Pencurian Privasi Big Data Di Era Industri 4.0. Jurnal Kajian Stratejik Ketahanan Nasional, 3(2). https://doi.org/10.7454/jkskn.v2i2.10042

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika*, *25, No. 01*(01). http://journal.ubaya.ac.id/index.php/yustika

Mutaqin, R., Sahary, F. T., Mutaqin, G., & Dharmopadni, D. S. (2023). Peran Disinfolahtad dalam Mempercepat Transformasi Digital di Lingkungan TNI AD. *Jurnal Academia Praja*, *6*(2), 229–244. https://doi.org/10.36859/jap.v6i2.1732

Niagahoster. (2021). *Apa Itu Big Data? Konsep, Karakteristik, dan Manfaatnya Bagi Bisnis Anda*. From Https://Www.Niagahoster.Co.Id/Blog/Bigdata-Adalah/.

ODNI. (2019). *What is Intelligence?* Https://Www.Dni.Gov/Index.Php/What-We-Do/What-Is-Intelligence.

Putro, T. W. A. (2024). Implementasi Big Data dan Artificial Intelligence Untuk Meningkatkan Kemampuan Intelijen TNI. Ranah Research: Journal of Multidisciplinary Research and Development, 6(6), 2864–2872. https://doi.org/10.38035/rrj.v6i6

Sarjito, A. (2023). Integrating the Concept of Situational Leadership and V.U.C.A. in Formulating Adaptive and Responsive Defense Policies. *Journal of Social Interactions and Humanities*, *2*(3), 221–238. https://doi.org/10.55927/jsih.v2i3.6229

Sarjito, A. (2024). Peran Intelijen Melalui Perumusan Kebijakan Pertahanan Negara dalam Perang Hibrida. *PANDITA: Interdisciplinary Journal of Public Affairs*, *7*(1), 74–88. https://doi.org/10.61332/ijpa.v7i1.152

Satar, M., & Yusri, N. A. (2019). Pengambilan Keputusan Ditinjau dari Manajemen Diri dan Kematangan Emosi. *Jurnal Al-Qalb*, *10*, *No. 1*, 20–41.

Yang, C., Yu, M., Li, Y., Hu, F., Jiang, Y., Liu, Q., Sha, D., Xu, M., & Gu, J. (2019). Big Earth data analytics: a survey. *Big Earth Data*, *3*(2), 83–107. https://doi.org/10.1080/20964471.2019.1611175.