International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 3, Number 1, August 2023, *Page. 431 - 440*
Email : editorijhess@gmail.com

Identify Cyber Intelligence Threats in Indonesia

Abdillah Satari Rahim[1)], Pujo Widodo[2)], Agus H.S. Reksoprodjo[3)], Alsodiq[4)]*
[1,2,3,4)] Asymmetric Warfare / Faculty of Defense Strategy, The Republic of Indonesia Defense University

*Corresponding Author
Email: abdillahsatarir@gmail.com, pujowidodo78@gmail.com, yono@sintesagroup.com, alsodiq.007@gmail.com

Abstract

Currently, the cyber domain has become a new strategy that can cause losses that have a strategic impact on a country. The current condition shows that the cyber domain has also been used in intelligence operations. The lack of human resource support, infrastructure support and financial support raises concerns about the readiness to deal with cyber intelligence threats in Indonesia. This research aims to analyse the identification of cyber intelligence threats in Indonesia. This research was conducted using a qualitative method with a case study approach. The analysis was conducted comprehensively through in-depth analysis of the issues raised. The results of this study show that the pattern of cyber intelligence threat identification in Indonesia focuses on deepening the aspects contained in the 9 components of strategic intelligence so as to produce estimates and early detection of potential threats / impacts that can be caused by cyber threats. So that it is necessary to increase information security awareness for the community and the need to increase the quantity and quality of human resources and infrastructure to support the success of cyber intelligence operations so as to produce quality intelligence products.

Keywords**: **Threat, Intelligence, Cyber

INTRODUCTION

War is essentially a situation where two or more countries are involved in an armed dispute accompanied by a statement of intention from the other party to dominate a contested area to impose peace conditions as desired by the winner (SESKOAD, 2019). In today's modern era, physical strength is no longer a priority in achieving victory, the comparison of the number of personnel and weapons is no longer relevant to be used as an indicator of strength (Supartono, 2017). The war paradigm that has emerged in various parts of the world today and in the future is the emergence of the phenomenon of abstract war or asymmetric warfare. This war occurs without the mobilisation of troops whose implementation is more directed towards technological and industrial superiority (SESKOAD, 2019). Knowledge and mastery in the field of information and communication technology (ICT) are problems faced in defending and protecting state sovereignty today.

This change in the strategic environment has led to a shift in the threat paradigm that is difficult to predict both globally, regionally and domestically. The Defence White Paper of the Republic of Indonesia (2015), explains that the threats faced by the country today and in the future are acts of terrorism and radicalism, separatism and armed rebellion, natural disasters, border area violations, piracy and theft of natural resources, disease outbreaks, cyber attacks and espionage, drug trafficking and abuse and open conflict or conventional warfare. Peacetime competition is a new challenge that can directly affect national interests and security, including ideology, politics, economy, socio-culture, defence and security, as well as geography, demography and natural resources. Improving the ability to collect and analyse information about the development of the strategic environment is currently a problem faced in protecting the country from various threats faced.

Specifically for cyber threats, the Defence White Paper of the Republic of Indonesia (2015), states that today cyber warfare has become a new strategy that can cause losses that have

a strategic impact on a country. One example faced today is the action of cyber terrorists, cyber propaganda, and proxy war where cyberspace is used to build control and coordination communication system channels, collect financial resources, recruit computer experts (hackers) to be used as cyber troops to create their cyber weapons (Gultom, 2017). Identifying as early and as detailed as possible all forms of threats such as strength, plans, and potential actions that will be carried out by certain actors in cyberspace is a problem faced today.

It cannot be denied that the presence of globalisation has many complex implications for human life and state relations today (Djoyonegoro, 2018). The rapid advancement of science and technology that accompanies the process of globalisation has given birth to various new means of communication through the internet media. On the one hand, the internet has currently provided many conveniences for humans in communicating, learning, working, and social interaction (Hadi et al., 2020). On the other hand, the internet has also been widely used by state actors and non-state actors to commit crimes (cybercrime) both physically and psychologically, which if the escalation continues to increase, can threaten the safety of the nation, territorial integrity and state sovereignty (Soewardi, 2013). In response to this, the supervision and control of internet communication facilities presented in the era of globalisation is a new problem that needs to be done in preventing various threats that may be posed.

The massive use of internet technology has increased the vulnerability of state security in cyberspace (cyber threat). Suratman (2017) explains that cyber threats have become a form of threat whose development rate has increased very rapidly in the last decade. This is evidenced by the following data on cyber attack trends in Indonesia:

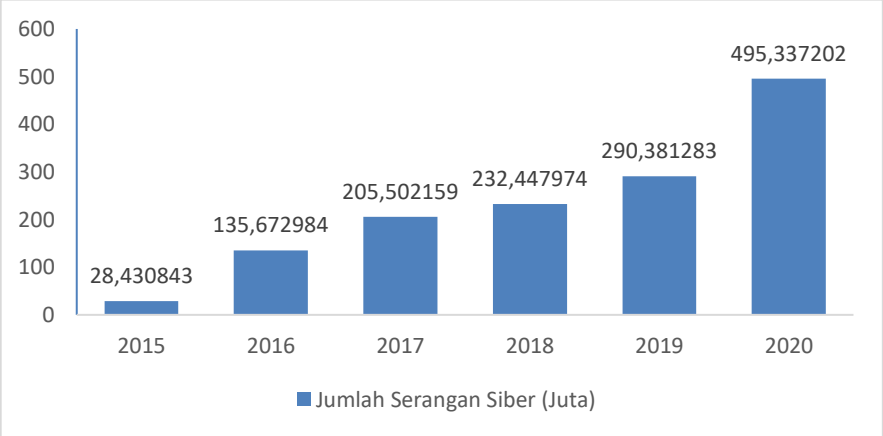

Chart 1. Cyber Attack Trends in Indonesia
Source: processed by researchers, 2022.

The lack of a comprehensive cyber security and defence governance policy in the form of a cybersecurity policy, cybersecurity strategy, and cybersecurity framework is the biggest unresolved problem to date.

The utilisation of cyberspace as a new alternative to delivering threats is considered an effective means. Setyawan and Sumari (2016) explained that cyber threats are currently widely used because of their wide scopes, such as stealing information, spreading destructive ideas, and launching attacks on information systems in all fields such as banking information, intelligence networks, and military and national defence systems. The lack of guidelines for countermeasures against various types of threats and different methods of cyberattacks is a separate problem faced today.

This poses challenges for national security and defence. One of the emerging issues is the concern that cyberspace has also been utilised by intelligence actors from both state and non-state actors. Hendropriyono (2013) explains that the threat intelligence faces in the future and can pose in cyberspace is opinion formation. In this case, the object of war is no longer the state,

but the human brain. The subject of war is no longer the army, but all the universal power of each party. The real example faced today is the emergence of the threat of radicalism ideology. Reporting from the official website of the KEMENDAGRI Research and Development Agency (2018) states that, currently, exposure to radicalism through social media content is widely circulated 24 hours without stopping. There are more than 200 channels that contain radical content on Telegram, which contains a rejection of diversity to invite violence, including against government officials in the name of religion. Each channel disseminates 80-150 radical messages every day with the average exposed person subscribing to 5-10 channels. This means that people can potentially be exposed to 1000 messages containing radicalism content per day. Intense media and opinion mobilisation without ignoring the freedom of the press that is carried out in a patterned and comprehensive manner is a new problem that must be mastered by intelligence agencies in Indonesia. In this case, the key is not only to react and counter misinformation but to take the initiative to build a favourable public opinion (Hendropriyono, 2013).

On the other hand, the threat of theft of strategic information is also a form of serious threat faced in the intelligence field (Hendropriyono, 2013). Various cases experienced such as the theft of Indonesian population data information, intrusion into the server or internal network of the State Intelligence Agency (BIN) and nine other state institutions, the action of tapping the President's telephone connection and important state officials, are small examples of various cyber intelligence threats that occur in Indonesia (Liputan6, 2021; Faisal Javier, 2021; Djoyonegoro, 2018). From the various examples of cases above, the management of cyber intelligence should be an integral part of intelligence analysis and activities so that the space for actors who want to damage and destroy the country both inside and through cyberspace can be suppressed. In response to this, understanding and placing the context of cyber intelligence in national intelligence governance is a new issue that needs to be developed by intelligence agencies in Indonesia.

Looking at the current conditions, the discussion on the placement of cyber intelligence threats in the governance of defence policy in Indonesia still has many weaknesses and obstacles. The biggest problem faced is the absence of a comprehensive regulation that can be used as a legal umbrella for security and defence stakeholders in Indonesia. This makes BAIS TNI and also BIN have limitations in carrying out their roles and functions as intelligence agencies in Indonesia.

Another problem faced by BAIS TNI and BIN is the readiness of human resources, infrastructure, funds and also qualified technology (Astarini & Rofii, 2021). In the aspect of human resources, Astarini (2021) explained that the ability of human resources in conducting cyber intelligence activities through collecting and processing intelligence data in and through cyberspace must be able to produce accurate and quality intelligence information. Accuracy in analysing existing information is needed considering the fast and dense flow of information in cyberspace will be difficult to stem.

Meanwhile, the ability of human resources to operate the various supporting infrastructure used is also needed. However, research conducted by Telstra and The Economist Intelligence Unit (2017) shows that limited talent and skills are the toughest digital challenges faced by Indonesia at 36%, surpassing limited investment funding (31%), low access to a robust technology ecosystem (20%), government policies or regulations (17%), and other cybersecurity issues (15%). This shows that increasing the capacity and capability of intelligence professionals as the first line of defence in carrying out their duties and functions in cyberspace is a major issue that needs attention.

On the aspect of technology and infrastructure, Ardiyanti (2014) explains that the complex scope of cyber handling requires the development of adequate infrastructure. The infrastructure referred to in this case is a technology consisting of hardware and software needed to protect

systems and data from external and internal cyber threats (Islami, 2018). Fitriati (2018) further explained that in the context of implementing national cyber defence, the preparation of technological recommendations leads to general and normative recommendations that prioritise the independence of domestic products including open technology architecture, the use of domestic ICT products or developed domestically, the development of open source technology solutions, and making maximum use of domestic human resources. In this case, cyber defence institutions require technological/infrastructure support in the form of supporting facilities such as buildings or data centre locations, Network Operation Centres (NOCs), laboratories, data centres and recovery centres, data networks, cyber defence administrative applications, cyber defence technical applications, and special technologies. The current condition shows that Indonesia's defence industry's capability in producing and developing hardware and software related to information technology is still very weak (Ardiyanti, 2014). The problem of information technology development is caused by several factors (KEMENKUMHAM, 2011):

a. Although the government has carried out industrial and manufacturing development since 1960. However, the quantity and quality (technical) development of information technology is still not running effectively.
b. The existence of a national legal umbrella in the form of laws and regulations governing the country's strategic industries to encourage the revitalisation of more concentrated national strategic industries is still temporary and incomplete.
c. The most concerning thing of all is that most of the procurement of information and communication technology comes from abroad, where the purchase funds are financed by foreign loans. When the government issues a policy to reduce the proportion of foreign loans, it will certainly have an impact on the development of the country's defence industry.

Furthermore, the cost and funding aspect also raises its problems. This is because seriousness in responding to various cyber threats requires enormous incentives (Ardiyanti, 2014). On the other hand, (Astarini & Rofii, 2021) added that in terms of the implementation of infrastructure and technology procurement which is one of the causes of progress and increasing the strength and capability of cyber defense in Indonesia has not been realized.

From this, it can be understood that the support capacity and capability of domestic infrastructure and technology are currently not able to meet the needs required by government agencies and non-ministerial institutions including intelligence in carrying out the function of national defence in cyberspace.

RESEARCH METHODS

This research uses a qualitative research method with a case study approach. The paradigm of this research uses the constructivism paradigm with an inductive way of thinking, starting from reality (das sein) and ending with hope (das solen). Sugiono (2017) explains that qualitative research is research that aims to find, analyze and manage direct events in the field by understanding social interactions with interviews and documentation. Meanwhile, Luthfiyah & Fitrah (2018), explained that qualitative research is a type of research that uses descriptive data in the form of oral and written communication obtained from the subject or object studied. Data collection in a qualitative method is carried out by studying the perspectives of participants through interactive and flexible strategies. in determining informants who will be interested in information in the data collection process in this study, researchers used purposive sampling techniques. The informants in this study are BAIS TNI institutions with BIN. The object of this research is the identification of cyber threats in Indonesia. Data was collected using interview techniques, documentation and literature study. Source triangulation, and data triangulation are

used in data processing to verify the accuracy of the data that has been taken. Data analysis was carried out referring to the concept of data analysis model Miles et al (2014).

RESULT AND DISCUSSION

The utilisation of cyberspace as a new alternative to providing threats is considered an effective tool. Setyawan and Sumari (2016) explained that cyber threats are currently widely utilised because of their wide and dynamic scope. This is a problem in itself considering that cyber threats are currently also one of the main concerns in the intelligence world. Hendropriyono (2013) explains that the intelligence threat faced in the future and can be posed in cyberspace is opinion formation. In this case, the object of war is no longer the state, but the human brain. The subject of war is no longer the army, but all the universal power of each party.

On the other hand, the threat of theft of strategic information is also one of the serious threats faced in the field of intelligence (Hendropriyono, 2013). Various cases experienced such as the theft of information on Indonesian population data, the act of infiltration into the server or internal network of the State Intelligence Agency (BIN) and nine other state institutions, the act of tapping the President's telephone connection and important state officials, are small examples of various cyber intelligence threats that occur in Indonesia (Liputan6, 2021; Faisal Javier, 2021; Djoyonegoro, 2018). This peacetime competition is a new challenge that can directly affect national interests and security, including ideology, politics, economy, socio-culture, defence and security, as well as geography, demography, and natural resources.

Therefore, the recognition and/or identification of threats and potential threats in cyberspace should be an integral part of intelligence analysis and operations so that the space for actors who want to damage and destroy the country both in and through cyberspace can be suppressed. In this case, the ability to recognise and identify various cyber intelligence threats is an important aspect that must be owned by intelligence agencies as a consideration in producing quality intelligence products to support national defence. The ability to conduct a good threat analysis becomes a benchmark in producing intelligence products that are measurable, effective and do not adversely affect other aspects.

The relationship between the identification of cyber intelligence threats in Indonesia and this research is because the threat of cyber intelligence in Indonesia has now become one of the forms of threats that must be recognised, understood and controlled by intelligence agencies in Indonesia. Thus, intelligence agencies in Indonesia, in this case, BAIS TNI and BIN, can carry out prevention and early detection so that cyber intelligence threats in Indonesia do not have an impact that can disrupt or damage state sovereignty.

Based on the results of interviews conducted at the National Intelligence Agency with Mr Kombespol. Agung Marlianto, S.ik., M.H. as Head of the Sub directorate of Personnel Administration of Deputy VI BIN on 31 May 2022, related to the cyber intelligence threat paradigm in the perspective of BIN, the following results were obtained

The weakness of the defence system and network infrastructure security is one of the causes of the rampant cyber attacks on government and private institutions. As with the latest incident related to the leakage of protected care data, the mustang panda hacker group with its thanos malware managed to enter into 10 K / L, the rise of hoax news on social media platforms, not to mention the rampant spread of extremism and radicalism on social media shows that Indonesia is currently not so strong in terms of national cyber security. (Head of Personnel Administration Subdirectorate of Deputy VI BIN, 31 May 2022).

Based on the results of data verification and validation conducted through both source triangulation and method triangulation techniques related to the identification of cyber

intelligence threats in Indonesia by the National Intelligence Agency. It can be understood that the data collected through the first informant has the same substance as the data collected through other supporting informants and is supported by related documents that serve as comparative data. Thus, the data that has been obtained can be used as material for research analysis.

Based on the results of interviews related to the cyber intelligence threat paradigm in Indonesia from the perspective of BAIS TNI conducted with the Deputy Commander of the Geospatial & Informatics Intelligence Unit of BAIS TNI, Colonel Sus. Rifki Indra Kusuma, S.T., M.Sc. on 28 July 2022 as the first informant, the following results were obtained

Based on the results of data verification and validation carried out both through source triangulation techniques and method triangulation related to the identification of cyber intelligence threats in Indonesia carried out by BAIS TNI. It can be understood that the data collected through the first informant has the same substance as the data collected through other supporting informants and is supported by related documents that have been collected previously. Although there are answers and/or information that contradict the data obtained from the main informant, when looking at the substance of other supporting data, the validity of the data obtained from the first informant can be proven. Thus, the data that has been obtained can be used as material for research analysis.

From the results of the data processing above, it is found that BAIS TNI through the Commander of the Geospatial and Informatics Unit of BAIS TNI views that the current shift in the strategic environment has also had an impact on shifting the threat paradigm by utilising the digital world that is interconnected to the internet. This, if used and/or exploited in intelligence activities or operations, can pose threats and/or potential threats that can harm the security and sovereignty of the state.

Related to the method used by BAIS TNI in identifying cyber intelligence threats in Indonesia, it is found that BAIS TNI through the Commander of the Geospatial and Informatics Unit applies four steps of threat recognition to classify various threats or potential threats that can be posed in or through cyberspace. Threat identification activities carried out by BAIS TNI are carried out by focusing on the implementation of intelligence stages (intelligence cycle). From these intelligence phases, it can be seen the losses or potential threats that can be posed in or through cyberspace.

Based on the findings obtained from the results of data processing, researchers conducted an analysis to determine the comparison of the methods used by the two institutions in identifying cyber intelligence threats in Indonesia. From the analysis conducted, it was found that both institutions have the same perspective regarding the nature of threats that can be posed by the cyber domain today. Both institutions consider that the cyber domain has been widely utilised in the implementation of intelligence activities and/or operations. Whether it is as a means of supporting intelligence activities and/or operations or as the main target of intelligence activity and/or operations. In general, the cyber intelligence threat identification activities carried out by the two institutions are similar both in terms of assessment indicators and threat identification methods. In the aspect of threat classification indicators, it refers to the depth of aspects contained in the 9 components of strategic intelligence which include ideology, politics, economy, society and culture, defence and security, geography, demography, history, and biography of prominent figures. Meanwhile, the threat identification method refers to the four steps of threat classification as outlined in the Indonesian Defence White Paper, which includes threat analysis, threat classification, threat targets, and threat escalation.

Although both institutions have different main tasks where BIN as mandated by the Law has the main task of preventing and early detection of various threats and potential threats that can disrupt national interests and security from within and outside the country. Meanwhile, BAIS TNI has the main task of carrying out defence and/or military intelligence functions in supporting

the TNI's main task. However, in terms of function and purpose, both institutions have similarities, namely conducting investigations, security or counter, and raising intelligence aimed at detecting, identifying, assessing, analysing, interpreting, and presenting Intelligence to provide early warning to anticipate various possible forms and nature of potential and real threats to the safety and existence of the nation and state as well as opportunities that exist for national interests and security (Law Number 17 of 2011 concerning state intelligence).

The cyber domain has now been widely utilised in the implementation of intelligence activities and/or operations. Whether it is as a means of supporting intelligence activities and/or operations as the main target of intelligence activity and/or operation. Therefore, in general, cyber intelligence threat identification activities carried out by both institutions have similarities in terms of both assessment indicators and threat identification methods.

In the aspect of threat classification indicators, it refers to the depth of aspects contained in the 9 components of strategic intelligence which include ideology, politics, economy, society and culture, defence and security, geography, demography, history, and biography of prominent figures. Meanwhile, the threat identification method refers to the four steps of threat classification as outlined in the Indonesian Defence White Paper, which includes threat analysis, threat classification, threat targets, and threat escalation. Although the two institutions have different main tasks as mandated by the Law, they have the main task of preventing and early detection of various threats and potential threats that can interfere with national interests and security from within and outside the country. However, both of them have similar functions and objectives, namely conducting investigations, securing or countering, and raising intelligence aimed at detecting, identifying, assessing, analysing, interpreting, and presenting Intelligence to provide early warnings to anticipate various possible forms and nature of potential and real threats to the safety and existence of the nation and state as well as opportunities that exist for national interests and security (Law Number 17 of 2011 concerning state intelligence).

For its application in the field, the two institutions must divide the scope of threats in accordance with their respective tasks and functions specifically tailored to the type of threat faced. For BAIS TNI, it is more directed towards military threats, while BIN is more directed towards non-military threats. Thus, the two institutions have the responsibility to coordinate and complement each other. Because both BIN and BAIS TNI both have the authority to carry out their functions as organising state intelligence institutions against these threats.

This refers to the definition of every threat that arises requires rapid anticipatory action so as not to cause harm to the nation. However, countermeasures require different actions for each threat. Therefore, there are four steps of threat recognition to be able to classify the threats that arise according to their type. the four steps are analysis, classification, targeting, and threat escalation (Ministry of Defence of the Republic of Indonesia, 2015).

Researchers view that BIN and BAIS TNI can analyse threats well. The ability to analyse threats is identified comprehensively and systematically. Seeing and describing in detail the various threats that arise from a number of dominant factors, both external factors and internal factors. External factors relate to actors or perpetrators who have intentions, goals, and indications. Internal factors are factors that facilitate or provide space for threats to occur, both static and dynamic.

After identifying these factors, threats can be classified according to the type, source and actor of these threats. Based on the type, national defence threats are classified into military threats, non-military threats and hybrid threats. When viewed from the source, the threats faced by Indonesia can come from abroad and within the country. Meanwhile, based on the actors, threats can be carried out by state actors or non-state actors, aka it could consist of an individual or a certain group. As a result, these threats can systematically threaten the sovereignty of the state, the territorial integrity of the Republic of Indonesia and the safety of the entire nation.

Of the various threats that arise, of course, the main target of these threats leads to state sovereignty. It can be in the form of control or occupation of part of the land, sea and airspace or claims to Indonesian territory/islands made by other countries. Therefore, there are conflicts or disputes between countries that can be categorised as threats to state sovereignty. As a result, the territorial integrity of the Republic of Indonesia can be partially, or fully lost on the ownership of the sovereign territory of the Republic of Indonesia.

These things can happen because of the desire to be independent or separate from the Republic of Indonesia carried out by non-state actors who have the support of state actors or third parties which can also be categorised as threats to territorial integrity. The target of threats to the safety of the entire nation can be in the form of threats to the safety of the body and soul of every Indonesian citizen, both at home and abroad, as a result of physical or non-physical actions from state actors and/or non-state actors.

Seeing these things, researchers see that there will be potential for threat escalation that comes suddenly and urgently. The escalation process can occur from the lowest to the highest. TNI elements and each ministry/institution will take part in each stage. The escalation is adjusted to the dynamics of the developing threat which is handled through the levels of the situation, both in military threat escalation and non-military threat escalation. Threat escalation starts from low, medium and high conditions. The escalation of military threats from within begins with civil order, a civil emergency and then becomes a military emergency based on the political decision of the state. Meanwhile, the escalation of non-military threats is adjusted to the types and forms of threats that will affect the condition of national defence. The escalation that occurs is not always sequential but directly to conditions that require the handling of all components of the nation. The determination of high escalation is carried out by institutions that have authority over state security.

According to the understanding of Bahtiar et al (2021), BIN and BAIS TNI can classify cyber threats in Indonesia based on intelligence considerations. Of course, the threat grouping must be based on a certain scale, namely the minor (small), moderate (medium), serious (large) and critical (very large) scales. This can be a benchmark in the action of intelligence activities that are measurable, effective and do not adversely affect other aspects.

CONCLUSION

Based on the results of the research and discussion that has been carried out related to cyber intelligence threat identification in Indonesia, it can be concluded that BAIS TNI and BIN have implemented 4 threat identification classifications well. The cyber intelligence threat identification pattern carried out by both institutions focuses on deepening the aspects contained in the 9 components of strategic intelligence to produce estimates and early detection of potential threats/impacts that can be caused by cyber threats.

REFERENCES

Ardiyanti, H. (2014). "*Cyber-Security* Dan Tantangan Pengembangannya Di Indonesia". *Politico*, 5(1), hh. 95–110.

Astarini, Dwi. R. S., dan Rofii, M. S. (2021). "Siber Intelijen Untuk Keamanan Nasional". *Jurnal Renaissance*, 6(1), hh. 703-709. https://doi.org/10.53878/jr.v6i1.143.

Bahtiar, Andhi dkk. (2021). "Analisa Kewenangan Badan Intelijen Negara (BIN) dalam Penanagan Covid-19". *Jurnal Ilmiah Ilmu Pemerintahan (JIIP)*, 6(2), hh. 177-190.

Djoyonegoro, Ngasiman. (2018). *Intelijen di era digital : prospek dan tantangan membangun ketahanan nasional*. Jakarta: CMB Press.

Fitriati, Rachma. (2018). *Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara*, 2nd ed. Jakarta: Universitas Pertahanan Indonesia.

Gultom, Rudy. A. G. (2017). "Membangun Kemampuan Siber dan Persandian Nasional guna Mengantisipasi Tantangan Keamanan Siber di Era Globalisasi Informasi dalam Rangka Melindungi Keutuhan dan Kedaulatan NKRI". *Jurnal Kajian LEMHANNAS RI*, 30(9), hh. 23–36.

Hadi, Martano. D. S., Widodo, Pujo, dan Putro, Resmanto. W. (2020). "Analisis dampak pandemi Covid 19 di Indonesia ditinjau dari sudut pandang keamanan Siber". *Jurnal Kebangsaan*, 1(1), hh. 1–9.

Hendropriyono, Abdullah. M. (2013). *Filsafat intelijen Negara Republik Indonesia*. Jakarta: Kompas Media Nusantara.

Islami, Maulia. J. (2018). "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index". *Jurnal Masyarakat Telematika Dan Informasi*, 8(2), hh. 137-144.

KEMENDAGRI, Badan.L. (2018). Hasil Studi: Penyebaran ISIS di Indonesia Makin Cepat Lewat Telegram". Retrieved from http://litbang.kemendagri.go.id/website/hasil-studi-penyebaran-isis-di-indonesia-makin-cepat-lewat-telegram/, pada 14 November 2021.

KEMENKUMHAM, B. (2011). Laporan Akhir Tim Pengkajian Hukum Tentang Pengembangan Dan Pemanfaatan Industri Strategis Untuk Pertahanan. Jakarta: Kementerian Hukum dan Hak Asasi Manusia.

Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia*. Jakarta: Kementerian Pertahanan Republik Indonesia.

Liputan6. (2021). "Data 279 Juta Penduduk Indonesia Diduga Bocor dan dijual di Forum Online". Retrieved from https://www.liputan6.com/tekno/read/4562268/data-279-juta-penduduk-indonesia-diduga-bocor-dan-dijual-di-forum-online, pada 14 November 2021.

Luthfiyah, dan Fitrah, M. (2018). Metodologi Penelitian; Penelitian Kualitatif, Tindakan Kelas & Studi Kasus. Sukabumi: Jejak.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis, A. Methods Sourcebook, Edition 3*. New York: Sage Publications.

SESKOAD. (2019). Kajian Tentang Konsekuensi Logis Perkembangan Globalisasi dan Kemajuan IT Terhadap Kepentingan Organisasi TNI AD. Bandung: Sekolah Staff Angkatna Darat.

Setyawan, David. P., dan Sumari, Arwin D. W. (2016). "Diplomasi Pertahanan Indonesia dalam Pencapaian *Cybersecurity* Melalui *ASEAN Regional Forum On Cybersecurity Initiatives*". *Jurnal Penelitian Politik*, 13(1), hh. 1-20. https://doi.org/https://doi.org/10.14203/jpp.v13i1.250

Soewardi, Bagus. A. (2013). "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia". Potensi Pertahanan / Media Informasi DITJEN POTHAN KEMHAN, hh. 31–35.

Sugiyono. (2017). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabet

Supartono. (2017). *Sistem Informasi TNI Dalam Rangka Interoperability Data Link Pertahanan Negara*. Bogor: Universitas Pertahanan Republik Indonesa.

Suratman, Yosua. P. (2017). "Penggunaan Strategi Operasi Kontra Intelijen Dalam Rangka Menghadapi Ancaman Siber Nasional". *Jurnal Pertahanan & Bela Negara*, 7(2), hh. 1–18. https://doi.org/10.33172/jpbh.v7i2.176.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.