International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 4, Number 2, October, *Page. 1176 – 1185*
Email : editorijhess@gmail.com

Integrated Defense: Merging Social Media, Cyber, and Technological Aspects in Asymmetric Warfare

Iwan Setiawan [1)], Fauzia G. Cempaka [2)], Yono Reksoprodjo [3)],
[1,2,3)]Asymmetric Warfare Study Program, Faculty of Defense Strategy,
The Republic of Indonesia Defense University, Indonesia

*Corresponding Author
Email: iwansetiawan7898@gmail.com / iwan.setiawan@sp.idu.ac.id

Abstract

Integrated defense is a core component of Indonesia's defense and security strategy, designed to protect the country's sovereignty, territorial integrity, and national safety from both physical and non-physical threats, especially cyber threats. With the rapid technological advancements and the rise of social media, cyber threats have become a significant concern as they impact various aspects of national security. Indonesia's large population of internet and social media users heightens the urgency for strategic attention to cyber defense. The government has introduced various policies and regulations, such as those by the Ministry of Defense, to strengthen cyber security and integrate it into national defense mechanisms. This study uses a qualitative descriptive approach, analyzing literature and legal frameworks to highlight the significance of integrated defense in addressing modern, asymmetric threats. In asymmetric warfare, non-military means, including cyber-attacks, are used to weaken a nation's ideological, political, economic, and social systems. The research emphasizes the need for a comprehensive and adaptive strategy, involving collaboration between the government, private sector, and civil society, to counter these complex threats. Strengthening cyber defense through education, training, and public awareness is crucial for safeguarding Indonesia's national security in the digital age.

Keywords: Cargo Parachutes, Logistics Distribution, Natural Disasters, Isolated Areas.

INTRODUCTION

Integrated defense is a strategic approach developed by the Indonesian government within the framework of its universal people's defense and security system (Sishankamrata) to safeguard national sovereignty, territorial integrity, and the safety of the nation from a variety of threats. These threats are characterized by populism, universality, and territoriality, with careful consideration given to changes in the global strategic environment (Ministry of Defense of the Republic of Indonesia, 2022). Integrated defense is designed to address both physical and non-physical threats, especially as technological advancements and the rapid spread of information reshape the security landscape. The advent of the internet has created a non-physical realm where people interact—most notably through social media—which has given rise to non-physical threats, commonly referred to as cyber threats (Arianto & Anggraini, 2019). These threats are not tangible, yet their impact is real and significant, particularly in terms of information and technology security, making them a critical component of cybersecurity.

The prevalence of social media and its profound influence on daily life is evident in the vast number of internet users, particularly in Indonesia. The country has 212.9 million internet users, of which 167 million are active on social media platforms. When compared to Indonesia's total population, this represents 77% of the population being internet users, and 60.4% of the population actively engaging with social media (WeareWearesocial, 2023). The potential negative impacts of social media and cyber technologies necessitate a strategic approach that balances innovation with national regulations designed to protect society. As such, the government, along with private sector and civil society actors, must focus on ensuring the security of information by enhancing cybersecurity measures. According to Rizki (2022), these

efforts include mechanisms for protecting the confidentiality, integrity, and availability of data, which are critical in minimizing disruptions. In response to these emerging challenges, the Indonesian government has enacted various policies and regulations aimed at bolstering cyber defense. Key measures include the Ministry of Communication and Information Technology (Permenkominfo) Regulation No. 5 of 2017, the Ministry of Defense (Permenhan) Regulation No. 82 of 2014, Presidential Regulation No. 53 of 2017 establishing the State Cyber and Crypto Agency (BSSN), Presidential Regulation No. 47 of 2023, and a series of BSSN regulations issued in 2021. These policies are supplemented by legislative actions, including Law No. 27 of 2022 and Presidential Regulation No. 95 of 2018. Despite the comprehensive regulatory framework, the successful implementation of these policies depends on strengthened collaboration among government bodies, private sectors, civil society, and national security and intelligence institutions, such as the Indonesian National Armed Forces (TNI), Indonesian National Police (Polri), BSSN, State Intelligence Agency (BIN), and the Strategic Intelligence Agency (BAIS).

Such cooperation is essential in addressing the complexities of modern life, where conventional national and international boundaries have become increasingly blurred. A new set of strategies and tactics is required to effectively respond to these challenges. This need is highlighted by the concept of asymmetric warfare, which views modern conflict as extending beyond the traditional military sphere to include non-military dimensions such as cyber threats. The complexity of contemporary warfare requires new concepts, strategies, and doctrines to deal with both military and non-military forces in a rapidly changing environment (Hendrajit, 2019). Asymmetric warfare, as described by former Indonesian Defense Minister Ryamizard Ryacudu, involves non-military methods employed by developed countries to weaken or destroy other nations by targeting key areas such as ideology, politics, economy, socio-culture, and security (Hendrajit, 2019). The scope of warfare has expanded beyond traditional military confrontations, and today, non-military actors have the ability to exert decisive influence on different battlefields, including cyberspace. Suryokusumo et al. argue that modern warfare is no longer limited to military engagements but involves a wide range of forces capable of shaping conflicts through non-traditional means (Hendrajit, 2019). This shift necessitates the involvement of non-military forces in addressing cyber threats as part of a broader integrated defense strategy.

Given the urgency of adapting to these modern threats, this paper emphasizes the need for a robust integrated defense framework that combines military and non-military capabilities, including cybersecurity, social media, and technological aspects. By incorporating these elements into the national defense strategy, Indonesia can effectively confront the complexities of asymmetric warfare. This approach not only enhances the nation's resilience against both physical and non-physical threats but also strengthens the overall defense of the Unitary State of the Republic of Indonesia (NKRI).

RESEARCH METHODS

This research method uses a descriptive qualitative method where the data collected is primary data and secondary data, namely by literature review, legal arguments and theories that support the research. Data collection according to qualitative research methods refers to the essence of a phenomenon, object and person where in this process includes observation, interviews or documents (Miles and Huberman 1994, 9). The data analysis technique used is the interactive model (Miles and Huberman 1994, 12).

Referring to the above understanding, data containing explanations related to integrated defense, cyber and technology and asymmetrical warfare are collected (data collection) first, whether in the form of books, journals, theses, theses or dissertations. The findings were then

analyzed qualitatively along with data presentation and reduction during the data collection process. The research discussion begins with a discussion of the concept of integrated defense, which will serve as an introduction to the discussion of the urgency of the concept of integrated defense in overcoming complex threats. Furthermore, the role and interrelationship of social media, cyber and technology will be discussed to find their influence on public opinion. The results of the discussion will be linked to asymmetric warfare by first briefly discussing the concept of asymmetric warfare to see the previous discussion in the context of asymmetric warfare. The last discussion is the implementation strategy derived from the linkage of the important points of the previous discussion as well as the conclusion of the discussion

RESULT AND DISCUSSION

The Urgency of Addressing Modern Threat Complexity

One of the characteristics of a country, in addition to the form of state, government system and political system is the military power that can be identified through the defense system. National defense for a sovereign nation is a way to maintain, protect and defend the integrity, unity and integrity, and sovereignty of the nation against all forms of threats. (Halkis, 2022). The defense system used by Indonesia involves all citizens, territories and other national resources that are prepared early by the government and organized in a total, integrated and directed, and sustainable manner to uphold state sovereignty, territorial integrity, and the safety of the entire nation from all threats. Such a defense system is then known as the Universal defense system (Halkis, 2022). Integrated defense is legally regulated in the general policy of national defense through Presidential Regulation No.7 of 2008 along with other defense policies, including defense implementation policies. (Central Government 2008). An explanation of the national defense implementation policy is explained in the Ministry of Defense of the Republic of Indonesia No.12 of 2021 that the implementation of defense is not only the responsibility of the Ministry of Defense and the Indonesian National Army (TNI), but all Indonesian people, both government agencies and non-governmental institutions and the community. (Ministry of Defense of the Republic of Indonesia, 2021). In an effort to realize integrated defense, the Minister of Defense encourages Ministries, Institutions, Regional Governments in an effort to utilize all resources to improve non-military defense capabilities (Kemhan RI 2022). The policy of organizing national defense which is then used in dealing with threats to national defense, both military and non-military in nature. (Kemhan RI, 2012).

Threats to national defense, especially non-military threats in their new forms, cause damage that is sometimes more than conventional threats. Modern threats to defense do not only involve military force. Ryamizard explained that the purpose of modern warfare is to eliminate the ability of the target country so as not to become a potential threat; weaken the ability of the target country so that it is increasingly dependent and easier to suppress; total control of the target country (Hendrajit, 2019). The target of non-military threats is not only one aspect but also various aspects, can be carried out simultaneously, or simultaneously with different intensities. Hendrajit explained that there are 3 (three) targets; first, deflecting a country's system according to the interests of colonialism; second, weakening ideology and changing the mindset of its people; third, destroying food security and energy security (guaranteed energy supply), and then creating dependence of the target country on these two things (food and energy security) (Hendrajit, 2019).

The complexity of modern life requires developing countries to face consequences, especially in the field of defense. The targets of threats to national defense are not only physical but also non-physical (re: digital, virtual), such as data and information connected through the

internet network where there are important and confidential data and information in it. Explanations related to modern threats and their 3 (three) targets definitively-intepretatively have similarities with cyber based on analysis through a modern framework of thought. Cyberspace or cyber is a space where communities are interconnected using networks (e.g. internet) to carry out various daily activities (Kemhan RI, 2016). Cyber threats are defined as all forms of actions, words, thoughts whether carried out by any party, with any motive and purpose, carried out in any location, based on electronic systems or their contents (information) or equipment that is highly dependent on technology and networks on any scale, against vital and nonvital objects in the military and non-military spheres, which threaten state sovereignty, territorial integrity and national safety (Kemhan RI, 2014).

Cyber threat indicators are divided into 3 (three) groups, first, hardware threat; second, software threat; third, data/information threat (Kemhan RI, 2014). Various indicators of cyber threats require the government, especially ministries / defense agencies to expand and strengthen the defense system in the cyber sector, in the sense that defense is not only limited and strengthened within the scope of government ministries / agencies, but also within the private sector and society. According to the Indonesian Ministry of Communication and Information as quoted by DataIndonesia.id (Widi, 2023) there were 35 cases of data leakage in Indonesia.

Source: DataIndonesia.Id, "Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor", dalam https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor, accessed on November 30, 2023.

Data leaks of 34 million personal data in the passports of Indonesian citizens (WNI), 19.56 million personal data registered with BPJS Employment Indonesia, theft of 1.5 terabytes (TB) of personal data of Bank Syariah Indonesia (BSI) customers through LockBit ransomware, 35 million personal data of MyIndiHome users, to 204 million personal data of the General Election Commission (KPU) Permanent Voter Data (DPT) leaked and traded by an anonymous account hacker named Jimbo for $74,000 or the equivalent of Rp.1.2 billion (Whichis.actually, 2023).

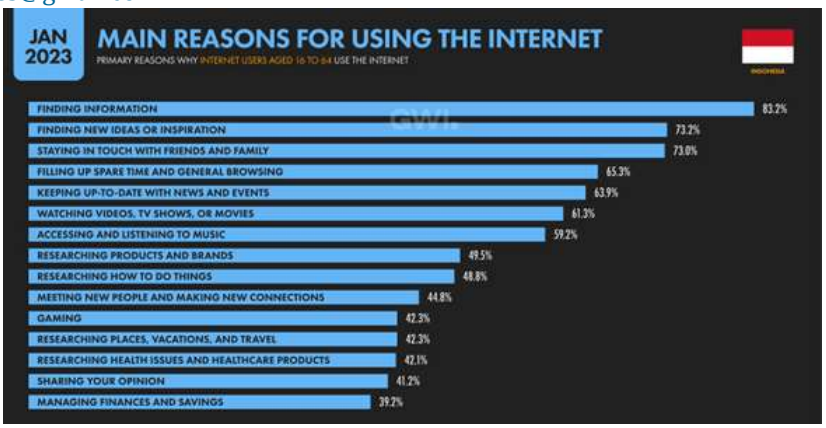
The phenomenon of online gambling is another cyber activity that is currently rampant and needs further attention, because the losses not only affect individuals but also the state morally. According to the Financial Transaction Reports and Analysis Center (PPATK) as quoted by dataindonesia.id (Rizaty 2023) there were more than 159 million transactions related to online gambling in Indonesia from January 1 - October 4, 2023 with a transaction value of Rp.160 Trillion. Compared to last year, the value of online gambling transactions in 2023 with a higher percentage, namely 52.69% to reach Rp.104.42 Trillion.

Source: DataIndonesia.Id, "PPATK: Transaksi Juni Online Cetak Rekor hingga Oktober 2023", dalam https://dataindonesia.id/varia/detail/ppatk-transaksi-judi-online-cetak-rekor-hingga-oktober-2023, accessed on December 02, 2023.

Based on reports of various cyber attacks that have an impact on the macro to micro scope of Indonesia, the government must strengthen the national defense system, especially in the cyber sector. Strengthening the defense system in the cyber sector can be started by providing education, such as promoting the implementation of education and training in the cyber sector. This is reflected in the annual report of the National Cyber and Crypto Agency (BSSN) through the development of national cyber and password security human resources, one of which is the Media Literacy and Cyber Security Movement (#JagaRuangSiber) which has been attended by 850,830 people (BSSN RI, 2023). Implementation can be carried out by the government through its agencies/institutions or in collaboration with private agencies/institutions involving the community. The implementation of this education is required in order to realize a comprehensive and adaptive integrated defense for Indonesia's cyber defense and security

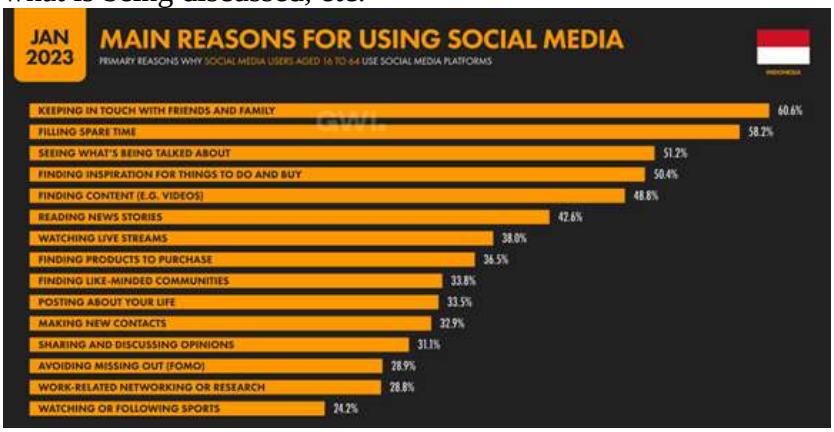
Social Media, Cyber, and Technology in the Context of Asymmetric Warfare

Social media as part of the development of cyberspace and technology has succeeded in changing the paradigm of social interaction among the community, starting from the method, to the style. The positive impact of the presence of social media, among others, does not limit the space and time of communication. Social media as new media plays a role in replacing the role of old media. Social media as new media is media that offers digitization, convergence, interactivity, and development of networks related to the creation and delivery of messages. (Watie, 2011). Social media changes and adds-even shifts-the world paradigm. The enthusiasm for the use of cyber and technological developments in Indonesia can be analyzed through the amount of internet usage, time spent and the use of technological devices to access it. We are Social provides an overview of this. It is known that there are 212.9 million internet users in Indonesia, which is 77.0% of the total population. The amount of time spent by each internet user in one day is 7 hours 42 minutes which is accessed through mobile phones as much as 98.3% (Wearesocial, 2023). We Are Social's Device Ownership data for 2023 (Wearesocial, 2023) shows that 99.4% of Indonesians own a smartphone which has increased by 3.5% every year, 61.7% own a laptop or computer which has decreased by -10.2% every year and 18.2% own a tablet which has increased by 1.1% every year. The main reasons for the large number of internet usage in Indonesia include searching for information, looking for inspiration or new ideas, connecting with family or friends, filling spare time, finding up to date news, etc. As described by We are Social in 2023.



Source: We Are Social 2023, "Digital Indonesia 2023", dalam https://wearesocial.com/id/blog/2023/01/digital-2023/, accessed on November 30, 2023.

Through social media, people can communicate anywhere, anytime and in any condition. The main reasons for using social media are interacting with family and friends, filling spare time, watching what is being discussed, etc.



Source: We Are Social 2023, "Digital Indonesia 2023", dalam https://wearesocial.com/id/blog/2023/01/digital-2023/, accessed on November 30, 2023.

Social media freely and openly allows individuals to express their thoughts and feelings, thus affecting social control which, in turn, affects the morality of the nation. Various conversations are merged in it. Something said by an individual or a group will be responded to directly, and at the same time what is uploaded will be seen, shared and even judged. Therefore, it is possible that an upload in the form of a message containing narratives becomes a propaganda tool that can influence public opinion. Departing from this proganda, it is impossible not to have a war.

Asymmetric warfare as a new (re: modern) style of warfare that tends to be non-violent (re: physical) is actually similar to conventional warfare patterns, but has differences in the nature and actions (Hendrajit, 2019). The bombardment phenomenon in conventional warfare is similar to asymmetrical warfare, namely through issues that are spread by related and involved parties in order to explode public attention and thinking. Then the phenomenon of the entry of cavalry troops, such as tanks and other armored vehicles in asymmetrical warfare is termed a theme or agenda to further penetrate public attention and thinking. Finally, the entry of infantry, in the cyber context, is to occupy, control and control the system adopted by the public, namely IPOLEKSOSBUDHANKAM (Hendrajit, 2019). If systematized, the stages in asymmetrical warfare are issues, themes, then schemes (Hendrajit, 2019). Another pattern worth looking at in asymmetric warfare is the proxy mode, which is a substitute, guardianship, or "puppet". In other

words, in carrying out this strategy, for example, it has individuals or groups who are asked or sent and subsequently rewarded so that they continue to act as substitutes or puppets.

Integrated Defense Implementation Strategy

The unavoidable reality of cyber development, especially social media, is that everything that is private and even confidential can become public consumption. More attention is needed from the government as state administrators, policy makers and other elements on aspects of cyber and technology, such as maximizing its positive use by increasing moral awareness in each individual. If not given more attention, it will slowly impact the morality of the nation. In the annual report of the National Cyber and Crypto Agency (BSSN), there is a Media Literacy and Cyber Security Movement program (#JagaRuangSiber). The program is one of the government's efforts in building national cybersecurity and password human resources. It is known that the program has been attended by 850,830 people (BSSN RI, 2023) consisting of junior and senior high school students, students, educators, santri / santriwati and the general public.

Through the ends, means, ways theory, integrated defense is aimed at securing national interests, including the protection of personal data of Indonesian citizens and residents, guaranteed access to information for each individual and the creation of formal channels as centers for communication, cooperation, coordination and collaboration on cyber issues. BSSN's National Cyber Security Strategy can be used as a strategic reflection on the implementation of integrated defense. Contemporary Cyber Architecture consists of 4 (four) interconnected defense devices, namely government, industry/private sector, society/community and academia. The connection between devices is built based on 5 basic principles, namely sovereignty, security, independence, togetherness, and adaptiveness. (BSSN, 2018)

The government as a state organizer plays a role in safeguarding, protecting and controlling the interests of the state. In order to strengthen the synergy of roles, academic tools are adjusted based on their academic background, such as coming from computer science, information technology, cyber media and asymmetric warfare majors. Cyber communities are classified based on ability, industry and type of social media, including cyber self-taught communities, white and gray hackers, social media communities, community cyber communities fostered by the government over the private sector and cyber industry communities, such as applications, infrastructure and infrastructure (BSSN, 2018). In the framework of asymmetric warfare, cyber control is driven by the cyber industry, as well as Cyber organizers. The movement of the cyber industry is monitored by the government together with academics and specialized cyber communities. The implementation outcome is to protect the country from all forms of cyber threats and disruptions.

CONCLUSION

The dynamics of modern warfare have implications for the warfare and defense strategies of every country. Asymmetric warfare is a fundamental challenge, complicated by the progress and development of technology, cyber and social media which currently have a central role. Such advances and developments have an impact on the living conditions of today's society, from lifestyle to paradigm. Modern warfare no longer makes the military the sole basis of national defense, so the involvement of civil society is a necessity. Therefore, a new defense strategy is needed that integrates all elements of the state to maintain state sovereignty and security. Integrated defense places the elements of the state to play a synergistic role according to their authority and capabilities. Considering that the cyber world is not a simple thing to deal with, it requires a comprehensive and adaptive division of roles and responsibilities. Within the framework of asymmetric warfare, the government mobilizes society through strategic policies

related to cyber. In order for strategic policies to be implemented well, a well-established implementation strategy is needed, so collaboration between government officials and private officials and the community is a must. Integrated defense promotes synergy-collaboration in order to maintain state sovereignty and security, especially in the aspects of cyber, social media and technology.

REFERENCES

Arianto, Adi Rio, dan Gesti Anggraini. 2019. "Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII)." Jurnal Pertahanan & Bela Negara (Universitas Pertahanan) Volume 9 Nomor 1: 13-29.

Bakhri, Syaiful Atim, and Yusuf Rizal Hanubun. n.d. "Pendekatan Kualitatif: Paradigma, Epistemologi, Teori dan Aplikasi." Sekolah Tinggi Agama Islam Negeri (STAIN) Sorong 1-21.

BSSN RI. 2021. "Peraturan Badan Siber dan Sandi Negara Nomor 3 Tahun 2021 Tentang Penyelenggaraan Literasi Media dan Literasi Keamanan Siber." Peraturan.go.id. Mei 19. Accessed November 11, 2023. https://peraturan.go.id/id/peraturan-bssn-no-3-tahun-2021.

—. 2021. "Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2021 Tentang Pelatihan Keamanan Siber dan Persandian." Peraturan.go.id. Juli 8. Accessed November 11, 2023. https://peraturan.go.id/id/peraturan-bssn-no-5-tahun-2021.

—. 2023. "Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023, BSSN: Materi Literasi Budaya Keamanan Siber dan Buktikan Akuntabilitas Kinerja." bssn.go.id. Februari 20. Accessed November 30, 2023. https://cloud.bssn.go.id/s/R7XkKdKjy4eFiQi.

BSSN. 2018. "Strategi Keamanan Siber Nasional." bssn.go.id. Agustus. Accessed Desember 6, 2023. https://www.bssn.go.id/wp-content/uploads/2018/08/Strategi-Keamanan-Siber-Nasional-signed.pdf.

Halkis, Mhd. 2022. Filsafat Ilmu Pertahanan: Suatu Pengantar. Bogor: Unhan Press.

Hendrajit, M. Arif Pranoto. 2019. "Perang Asimetris & Skema Penjajahan Gaya Baru." In Perang Asimetris & Skema Penjajahan Gaya Baru, by M. Arif Pranoto Hendrajit. Jakarta: Global Future Institute.

Kemhan RI. 2022. "Kebijakan Penyelenggaraan Pertahanan Negara Tahun 2020-2024 (JAKGARA HANNEG)." Kemhan.go.id. Agustus 26. Accessed November 29, 2023. https://www.kemhan.go.id/wp-content/uploads/2022/08/Permen-Jakgara-Hasil-Harmonisasi-tanggal-9-Maret-2021-roturdang-1.pdf.

Kemhan RI. 2015. Kebijakan Umum Pertahanan Negara Tahun 2015-2019. Kementerian Pertahanan.

—. 2009. "Peraturan Menteri Pertahanan Nomor 3 Tahun 2009 Tentang Kebijakan Umum Penggunaan Kekuatan Tentara Nasional Indonesia." Kemhan.go.id. April 8. Accessed November 11, 2023. https://www.kemhan.go.id/itjen/wp-content/uploads/migrasi/peraturan/permenhan%202009%20no%2003%20Kebijakan%20Umum%20Penggunaan%20Kekuatan%20Tentara%20Nasional%20Indonesia.pdf.

—. 2014. "Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber." Peraturan.go.id. Oktober 17. Accessed November 11, 2023. https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

—. 2012. "PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA NOMOR 03 TAHUN 2009 TENTANG KEBIJAKAN UMUM PENGGUNAAN KEKUATAN

TENTARA NASIONAL INDONESIA." Kemhan.go.id. Agustus 2. Accessed November 11, 2023. https://www.kemhan.go.id/itjen/2012/08/02/peraturan-menteri-pertahanan-republik-indonesia-nomor-03-tahun-2009-tentang-kebijakan-umum-penggunaan-kekuatan-tentara-nasional-indonesia.html.

—. 2021. "Peraturan Menteri Pertahanan Republik Indonesia Nomor 12 Tahun 2021 Tentang Kebijakan Penyelenggaraan Pertahanan Negara Tahun 2020-2024." Kemhan.go.id. Accessed November 11, 2023. https://www.kemhan.go.id/wp-content/uploads/2022/08/Permen-Jakgara-Hasil-Harmonisasi-tanggal-9-Maret-2021-roturdang-1.pdf.

—. 2016. "Permenhan No. 82 Tahun 2014 tentang Pertahanan Siber." Kemhan.go.id. Oktober 25. Accessed November 29, 2023. https://www.kemhan.go.id/pothan/2016/10/25/permenhan-no-82-tahun-2014-tentang-pertahanan-siber.html.

Kemkominfo RI. 2017. “Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2017 Tentang Perubahan Keempat Atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/per/m.kominfo/5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.” Peraturan.go.id. 19 Januari. Diakses November 27, 2023. https://peraturan.go.id/id/permenkominfo-no-5-tahun-2017.

KPU RI. 2022. "Keputusan Komisi Pemilihan Umum Nomor 12/TIK.03/14/2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025." jdih.kpu.go.id. Januari 2022. Accessed November 11, 2023. https://jdih.kpu.go.id/data/data_kepkpu/2022kpt012.pdf.

Miles, Matthew B., and A. Michael Huberman. 1994. An Expanded Sourcebook: Qualitative Data Analysis. London: Sage Publication.

Mustajab, Ridhwan. 2023. RI Alami 347,17 Juta Serangan Digital pada Semester I/2023. Juni 24. Accessed November 30, 2023. https://dataindonesia.id/internet/detail/ri-alami-34717-juta-serangan-digital-pada-semester-i2023.

Pemerintah Pusat. 2008. "Peraturan Presiden Nomor 7 Tahun 2008 Tentang Kebijakan Umum Pertahanan Negara." Peraturan.go.id. Accessed November 11, 2023. https://peraturan.go.id/id/perpres-no-7-tahun-2008.

—. 2018. "Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik." Peraturan.go.id. Oktober 2. Accessed November 11, 2023. https://peraturan.go.id/id/perpres-no-95-tahun-2018.

—. 2022. "Undang-undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." Peraturan.go.id. Oktober 17. Accessed November 11, 2023. https://peraturan.go.id/id/uu-no-27-tahun-2022.

Perpres. 2023. "Peraturan Presiden Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber." Peraturan.go.id. Juli 20. Accessed November 11, 2023. https://peraturan.go.id/id/perpres-no-47-tahun-2023.

—. 2017. “Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara.” Peraturan.go.id. 19 Mei. Diakses November 11, 2023. https://peraturan.go.id/id/perpres-no-53-tahun-2017.

Pertahanan, Kementerian. 2022. Kebijakan Pertahanan Negara Tahun 2022. Kementerian Pertahanan RI.

Rizaty, Monavia Ayu. 2023. PPATK: Transaksi Judi Online Cetak Rekor hingga Oktober 2023. Oktober 5. Accessed Desember 2, 2023. https://dataindonesia.id/varia/detail/ppatk-transaksi-judi-online-cetak-rekor-hingga-oktober-2023.

Rizki, Makbull. 2022. "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi." POLITEIA 54-62.

Social, We Are. 2023. "Digital 2023: Indonesia." We Are Social. January. Accessed November 11, 2023. https://wearesocial.com/id/blog/2023/01/digital-2023/.

Watie, Errika Dwi Setya. 2011. "Komunikasi dan Media Sosial (Communications and Social Media)." THE MESSENGER 69-75.

Whichis.sebenarnya. 2023. "KPU Dibobol Hacker, Data 204 Juta Warga RI Dijual di Internet." Instagram.com/Whichis.sebenarnya. November 30. Accessed November 30, 2023. https://www.instagram.com/p/C0RSdnCyrcy/?igshid=ZDE1MWVjZGVmZQ==.

Widi, Shilvia. 2023. Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor. Juli 6. Accessed November 30, 2023. https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.