International Journal of Multidisciplinary Approach Research and Science
E-ISSN 2987-226X
Volume 1 Issue 02, May 2023, Pp. 96-103
DOI: https://doi.org/10.59653/ijmars.v1i02.61

Digital Information Security Policy in the National Security Strategy

Asmadi [1], Hasan Almutahar [2], Sukamto [3], Zulkarnaen [4], Endang Indri Listiani [5], Agus Sikwan [6]

Universitas Tanjungpura, Indonesia | asmadi@fisip.untan.ac.id [1]
Universitas Tanjungpura, Indonesia | hasanalmutahar.untan@gmail.com [2]
Universitas Tanjungpura, Indonesia | sukamto@fisip.untan.ac.id [3]
Universitas Tanjungpura, Indonesia | zulkarnaen@fisip.untan.ac.id [4]
Universitas Tanjungpura, Indonesia | endang.indri.listiani@fisip.untan.ac.id [5]
Universitas Tanjungpura, Indonesia | agus.sikwan@fisip.untan.ac.id [6]

Received: 01-05-2023 *Reviewed: 05-05-2023* *Accepted: 25-05-2023*

Abstract

Security comes from the Latin word secure, significantly different from the dangers, fears, and threats associated with traditional and non-traditional security methods. Meanwhile, defense is defined as the most vital technology for the state in carrying out its national security function. National security is defined as the dynamic state of a country which covers all aspects of the nation's life in facing threats. National security includes protection for the state, society, and individuals. Until now, experts have provided several different definitions of the terms security and defense. This article analyzes the current digital information security threats in national security strategies and the implementation of adequate legal protections. This article applies a descriptive qualitative research approach by conducting document analysis. This article describes various information security threats in Indonesia, including disinformation, privilege escalation, and protection against phishing threats, data forgery, and card crime. The similarities and differences between the concepts of defense and security can be observed through regulations, the terminology used, institutions, and constitutions. This article shows that national information security is closely related to policy and closely relates to security, especially ITE policies. It cannot be separated that the security situation of a country depends on security and defense but synergistically with other factors, namely economic, political, legal, socio-cultural, ideological, geographical, and demographic.

Keywords: Digital information, Security, ITE Policy, National security, Strategy

Introduction

In the current technological and information development era, security threats are also increasingly complex. Even though infrastructure is getting more sophisticated to accommodate rapid changes, its presence places it in a critical position. Today everything in the world uses an almost fully developed infrastructure. Islami, M. J. (2017) states that the sophisticated infrastructure being built today is indeed vulnerable because it has the possibility of failure, which can be fatal. After all, society depends on the technology needed for their livelihood, which is responsible for many people. The increasingly tight integration of data centers and critical infrastructure, both physical and non-physical, into global networks and technologies exposes them to new security risks besides easy access and control. One of the causes of this risk is the threat of attacks from cyberspace that can penetrate information network systems and security against these important centers and infrastructure. Some criminal techniques are beyond the computer expert level, so network security cannot be guaranteed. The development of increasingly advanced technology indirectly influences the social behavior of Indonesian people, mainly social media users. The presence of social media allows people to easily discuss and share information. However, freedom of expression is also an essential part of people's lives within the framework of democracy. In this information and communicative era, information technology is increasingly accessible to the public. Ease of access to the Internet allows people to search, process, and receive information quickly. However, it also provides for disseminating unverified information without being filtered. There are two types of information sources, namely printed and non-printed or electronic, where information sources from the Internet are included in the category of non-printed information sources.

Non-printed sources of information via the Internet have various advantages, such as convenience, speed, and high accuracy. In addition, available capacity or free space, confidentiality, performance, and efficiency are essential factors that must be considered (Mahmudah, S, 2019). There are two types of information sources, namely printed and non-printed or electronic, where information sources from the Internet are included in the category of non-printed information sources. Non-printed sources of information via the Internet have various advantages, such as convenience, speed, and high accuracy. In addition, available capacity or free space, confidentiality, performance, and efficiency are essential factors that must be considered (Kornelius, 2019). There are two types of information sources, namely printed and non-printed or electronic, where information sources from the Internet are included in the category of non-printed information sources. Non-printed sources of information via the Internet have various advantages, such as convenience, speed, and high accuracy. In addition, available capacity or free space, confidentiality, performance, and efficiency are essential factors that must be considered (Kurniawan , N. A. 2014).

Not knowing the Internet existed so far, it has made life more accessible for people to interact without meeting in person. From a different perspective, the uncontrolled use of the Internet has resulted in the emergence of various criminal acts in cyberspace. Cybercrime or internet crime has become commonplace in many countries, including Indonesia. This crime first appeared in 1983 (Puspitasari, 2020). Cybercrime can be interpreted as actions carried out by specific individuals, groups, or entities using computers as tools to commit criminal acts or by making computers the target of these crimes (Munawar , Z. 2020). Online media in the current era is not only for conveying information but can also be used as a tool for political

propaganda to find positive and negative issues. Support from Facebook, Twitter, online media, and Instagram, of course, Social media can have a very positive impact, but on the other hand, it can also be a source of problems. Forum for expressing opinions, hate speech, and fake news (hoaxes). Not only fraud, common threats include denial of service (DoS) attacks in the form of synflood attacks and ICMP floods, phishing, and identity theft. In the current information and technology development era, security threats are also increasingly complex.

Besides that, the legal interest in protecting freedom of communication and access to information is also a constitutional right of citizens guaranteed. Crucial questions related to defamation and defamation according to the Criminal Code, the ITE Policy, and the provisions in the Criminal Code. Without realizing it, these issues can undermine the country's national security, so to protect freedom of speech and express opinions orally and in writing, the Information and Electronic Policy (UU ITE) must be able to safeguard various related legal interests. In addition, as a constitutional right of citizens, freedom of communication and access to information also needs to be protected by the ITE Policy based on Article 28F of the Constitution of the Republic of Indonesia (1945).

Meanwhile, the fundamental right to protect the dignity and good name of others also needs to be safeguarded, which is guaranteed by Article 28G(1) of the 1945 Constitution of the Republic of Indonesia. These legal interests must be regulated and limited by policy because everyone has responsibilities towards their society, and everyone can use their rights and powers only in a limited manner by policy, which is only aimed at the rights of others and to guarantee recognition and respect. These freedoms are based on Article 28J of the 1945 Constitution of the Republic of Indonesia.

Literature Review

Concept of National Security

Indonesia has various problems caused by internal and external factors. These internal factors often lead to conflicts of interest between the government and citizens, political parties, communities, indigenous peoples and religions, and individuals. Interested parties try to justify their expectations through various provocative means on social media and online media. The rise of false information in society can threaten the nation's diversity, unity, and integrity. External disputes can also occur due to overlapping foreign interests in Indonesia, either directly or indirectly. However, it cannot be denied that advances in science and information technology in building social relations between countries, and also as a means of exchanging information for the wider community.On the other hand, also create problems that destroy and level the interests of individuals, groups, and even actors and spread influence or achievements in information warfare. Particular interest in the use of information technology can be both negative and positive; information technology, if misused, can be a tool of destruction and a threat to the security of citizenship of the state and nation (Aji, 2022). Undeniably, the use of science and the development of information technology also create devastating problems, leveling the interests of individuals, groups, and even actors, spreading influence or achievements in the context of information warfare. Particular interest in the use of information technology can be both negative and positive; information technology, if misused, can be a tool of destruction and a threat to the security of citizenship of the state and nation (Sidik, 2013).

Undeniably, the use of science and the development of information technology also create

devastating problems, leveling the interests of individuals, groups, and even actors, spreading influence or achievements in the context of information warfare. Particular interest in the use of information technology can be both negative and positive; information technology, if misused, can be a tool of destruction and a threat to the security of citizenship of the state and nation (Rohmy, 2021).

Research Method

This study used the document analysis method with a qualitative approach. This qualitative research aims to investigate and describe in detail and thoroughly the conditions of a particular context with a descriptive approach, which reflects the natural situation in that environment and provides an in-depth understanding of what happened in the study field. In qualitative research, the object of research is natural. It comes from its natural environment, often referred to as a natural setting, so this type of research is known as naturalistic research. One method often used in conjunction with other qualitative methods is document analysis, which is helpful as a form of triangulation (Rohmy, 2021).

The specific stages in this research are as follows; Identifying the problem to be researched by the author, starting to get to know and be involved in the process and context of existing information sources, exploring various possible sources to obtain the information needed, starting to get involved with several (6 to 10) examples of documents relevant data, selecting units of analysis, creating protocols or coding forms and listing items or categories to guide data collection, as well as designing draft protocols or data collection sheets, testing protocols by collecting data from several existing documents, determining appropriate sampling methods and the strategy, be it theory based, cluster, or random stratification. Besides that, the process of determining to sample is also recorded for later reuse at the following data collection stage. In presenting data, you can include excerpts from interviews or narratives from observations made and make illustrations based on a summary of the information protocol for each case analyzed, all of which are done using critical thinking and analysis, combining all the results of data collection with the researcher's interpretation and critical concepts in different forms. The stages of the research above describe the document analysis research. This research also involved instruments and interviews, which will be discussed further in the next section. It can include excerpts from interviews or narratives from observations made and making illustrations based on a summary of the information protocol for each case analyzed, all carried out using critical thinking and analysis. Combining all data collection results with researchers' interpretations and key concepts in different forms.

The stages of the research above describe the document analysis research. This research also involved instruments and interviews, which will be discussed further in the next section. It can include excerpts from interviews or narratives from observations made and making illustrations based on a summary of the information protocol for each case analyzed, all carried out using critical thinking and analysis. Combining all data collection results with researchers' interpretations and key concepts in different forms. The stages of the research above describe the document analysis research. This research also involved instruments and interviews, which will be discussed further in the next section. The stages of the research above describe the document analysis research. This research also involved instruments and interviews, which will be discussed further in the next section. The stages of the research above describe the document analysis research. This research also involved instruments and interviews, which will be

discussed further in the next section.Digital Information Security Policy In The National Security Strategy.

Result and Discussion

Information technology in the concept of national security

In today's digital era, threats can be military or non-military. Military threats face enormous threats to the defense and security technology industry, such as; Cyber-attacks against military organizations and the like, while non-military threats can be in the form of a country's political, ideological, economic, and socio-cultural propaganda. Use of social media and online media. This is important in an era of rapid growth in technology flows. Filtering fraudulent information based on the concept of internal and external geopolitics (insular understanding) and geostrategy requires the attitude of relevant information technology management and decision-makers to recognize the fact that currently, most community activities are highly dependent on online systems, making internet connections interconnected in the cyber era.

On the other hand, inability or limited understanding of the ethical standards of social interaction in the online world and on social media often involves individuals or groups making use of developments in information technology properly, correctly, and effectively, which can cause social unrest and conflict in society. Indonesia's state defense is building the country's national strength through the regulation and control of welfare and security in a balanced way, in line with all aspects of people's lives and based on Pancasila, the 1945 Constitution, and its views. Based on this understanding, Archipelago cultural philosophy shows that the state's role in maintaining peace and harmony in the state for every citizen requires a complex and dynamic concept of national security so that Indonesia does not easily fall into the trap of fraud. The knowledge that develops in society, which can lead to social conflict, is approaching the dissolution of the nation. These aspects are always relevant and closely related to a country's national strength.

Astra Gatra consists of two interrelated aspects: Static Aspects (Tri Gatra) and Dynamic Aspects (Panca Gatra). Static Aspects include natural resources, geography, and demography, while Dynamic Aspects cover politics, economics, social culture, ideology, and defense and security. These two aspects are interrelated and influence each other (Kompas, 2022). We can all understand that these aspects are essential components and mutually influence one another.

The role of ITE policy in enforcing digital information security policies

Internet activity cannot be separated from the human factor, and its legal implications also intersect with humans in the physical world of society, triggering reflections on the need for legislation to regulate activities in cyberspace. (Al Jum'ah, 2018).

Because these characteristics vary widely, opinions arise for and against whether common policy can regulate cyberspace activities. This led to a discussion in the neighborhood. According to the Journal of Business Policy in 2010, the customary policy system based on the local legal system is deemed insufficient to deal with legal problems arising from human behavior in cyberspace. Besides that, in setting policys related to the Internet, two groups propose and consider the advantages and disadvantages of these regulations; first, the group completely rejects any attempt to regulate activities in cyberspace by policy (Chotimah, 2019).

The argument is that the Internet is a safe and democratic place that provides access to

free and open ideas and should not be constrained by rules based on conventional legal systems based on territorial boundaries. Second, the application of the system in general, the material for the ITE Policy is divided into two parts. The first part deals with data regulation and electronic transactions in the context of several international agreements, such as the UNCITRAL Model Policy on Uniform Trade and the UNCITRAL Model Policy on Electronic Signatures. The second part is the Rules for Prohibited Activities (Babys, S. A, 2019).

The ITE Policy itself has the following training objectives, improving the quality of providing broad opportunities for everyone to optimize their ideas and skills in the field of use and utilization of information technology with responsible responsibilities; and guarantee security, justice, and legal certainty for users and providers of information technology (Policy No. 11/2008, 2008) Cyberspace is an activity carried out through electronic media.

Even if it occurs in virtual media, activities in cyberspace can be classified as actual legal behavior. Legally, the category of cyber activity cannot be approached using only formal legal qualifications because this method is complicated and eliminates many legal aspects (Dammann, O., 2018). An activity in cyberspace is a. Electronic documents, such as the Electronic Commerce Act, are paper documents (Gulo, A. S., & Nawawi, S. L, 2020).

Therefore, special attention must be paid to ensuring legal certainty in using media, information, and communication to ensure that electronic commerce functions optimally. In order to close security gaps, the legal approach is fundamental so that all problems information technology etc. Policy No. 11 of 2008 concerning Information and Electronic Transactions stipulates eleven changes designed to facilitate electronic transactions, taking into account the principles of legal certainty, profit, prudence, and technology that are open and neutral, namely: The First Policy which describes the Use of Information Technology and Communications (ICT) and Electronic Information and Transactions (ITE), extraterritorial ownership; applies to all residents (D.N.) and foreigners (LN) which have legal consequences in the Unitary State of the Republic of Indonesia, produce legal guarantees for individuals who carry out transactions electronically, electronic legal evidence is recognized as other evidence under the Criminal Procedure Code (KUHAP), electronic signature (ITE) identified as traditional (ink and wet stamp), provides a formal legal definition of various matters regarding the use of information and communication technology (ICT), copies of documents or information stored in electronic or paper form are considered valid evidence and have legal effect, definitions of prohibited activities in the use of information and communication technology (ICT), enforce penalties for violations that occur, promote Indonesia's economic development as part of an information technology (I.T.)-based crime prevention strategy, and protect users of services that use information technology (I.T.). Everyone who acts following the policy, both within and outside the territory of Indonesia, will be subject to the same legal force as this trademark policy. However, if the action harms Indonesia's interests.

Conclusion

In the ongoing development of digital information and technology, security issues are increasingly complicated due to the threat of attacks from cyberspace that can damage information network systems and important security centers. This makes technological infrastructure even more vulnerable and critical because people depend on this technology for their lives. Nonetheless, information technology can be positive or negative depending on its use. Security threats, such as political, ideological, economic, and socio-cultural propaganda, can be military or non-military. Therefore, legal protection must be enforced to limit the incorrect use of information technology so as not to threaten the nation's diversity, unity, and integrity. ITE Policy in Indonesia However, the ITE Policy aims to improve the nation's standard of living, business development, and the national economy and provide the broadest possible opportunity for everyone. The ITE Policy has an essential role in maintaining information security and preventing the dissemination of information that can harm individuals or even the state. Because information and technology can affect the national interests of a country. The ITE Policy has provisions such as spreading false information or hoaxes, hacking, and theft of personal data. With the ITE Policy, which protects information and technology, information and technology security in Indonesia can be appropriately maintained. This can contribute to Indonesia's national security because information and technology are essential in maintaining the country's security and stability.

References

Aji, M. P. (2022). Sistem Keamanan Siber dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). 222-238.

Astriani, D. R., & Rofii, M. S. (2021). Siber Intelejen Untuk Keamanan Nasional. Jurnal Renaissance, 703-709.

Al Jum'ah, N. M. (2018). Analisa Keamanan dan Hukum Untuk Perlindungan Data Privasi. II(1), 39-44.

Babys, S. A. (2021). Ancaman Perang Siber DI Era Digital dan Solusi Keamanan Nasional Indonesia. Journal Oratio Directa, 425-442.

Chotimah , H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber dan Sandi Negara. Politica, 113-128. doi:https://doi.org/10.22212/jp.v10i1.1447

Dammann, O. (2018). Data, Informasi, Bukti, dan Pengetahuan : Proposal Untuk Informatika Kesehatan dan Ilmu Data. Jurnal Online Informatika Kesehatan Masyarakat.

Gulo, A. S., & Nawawi, S. L. (2020). Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. Pampas Journal Of Crime , 68-81.

Islami, M. J. (2017). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Indeks. 137-144.

Kornelius, Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. Refleksi Hukum, 145-160

Kurniawan , N. A. (2014). Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional . 1-14.Munawar, Z., & Putri, NI (2020). Computer Network Security in the Big Data Era. 14-20.

Kusumoningtyas, A. A., & Puspitasari. (2020). Dilema Hak Perlindungan Data Pribadi dan Pengawasan Siber : Tantangan Di Masa Depan . 234-

Mardhani, D., Runturambi, A. J., & Hanita , M. (2020). Keamanan dan Pertahanan Dalam Studi Ketahanan Nasional Guna Mewujudkan Sistem Keamanan Nasional . 279-297

Munawar , Z., & Putri , N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data . 14-20.

Nugroho, I. I., Pratiwi, R., & Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia. Iphmi Policy Journal, II(1), 115-129. doi:https://doi.org/10.15294/iphmhi.v1i2.53270

Nurpatria , B., & Ras , A. R. (2022). UU ITE : Kebebasan Berpendapat, Informasi Hoax Terhadap Ancaman Stabilitas Ketahanan Nasional. Jurnal Pendidikan Tambusai, II(6), 10220-10229

Purwantoro, S. A., Syahardani, R., Hermawan , E., & Damindarti , A. K. (2021). Media Sosial : Peran dan Kiprah Dalam Pengembangan Wawasan Kebangsaan. Jurnal Lembaga Ketahanan Nasional Republik Indonesia, IV(9), 55-79.

Radiansyah, I., Candiawan , & Priyadi, Y. (2016). Analisis Ancaman Phising Dalam Layanan Online Banking . 1-20.

Rahmatullah , I. (2021). Pentingnya Perlindungan Data Pribadi Dalam Masa Pandemi Covid-19 Di Indonesia . 11-16.

Rifauddin , M., & Halida , A. N. (2018). Waspada Cybercrime dan Informasi Hoax Pada Media Sosial Facebook. Jurnal Perpustakaan, Informasi, dan Kearsipan, 98-111. doi:https://doi.org/10.2452/kah.v6i2a2.

Rohmy, A. M., Suratman , T., & NIhayaty, A. I. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. Jurnal Dakwah dan Komunikasi Islam (7), 309-339.

Sebuah Kajian Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). (2011). JEAM, X(1), 43-48.

Sidik, S. (2013). Dampak Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Terhadap Perubahan Hukum dan Sosial Dalam Masyarakat. Jurnal Ilmiah WIDYA, 1-7.

Syed, R., Khawer , A. A., & Yasin , M. (2019). Cyber Security. 1-3. Diambil kembali dari https://www.jstor.org/stable/resrep24376.5