DINASTI RESEARCH

JLPH:
Journal of Law, Politic and Humanities

E-ISSN: 2962-2816
P-ISSN: 2747-1985

https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/jlph.v5i5

The Strategic Role of the National Cyber and Crypto Agency (BSSN) in Maintaining State Sovereignty in Cyberspace

Muhammad Prakoso Aji[1], Gumilar Rusliwa Somantri[2], Muhammad Syaroni Rofii[3].
[1]Universitas Indonesia, Indonesia, muhammad.prakoso21@ui.ac.id.
[2]Universitas Indonesia, Indonesia, gumilar.r29@ui.ac.id.
[3]Universitas Indonesia, Indonesia, muhammadsyaroni@ui.ac.id.

Corresponding Author: muhammad.prakoso21@ui.ac.id[1]

Abstract: The development of technology places data in cyberspace as a very valuable commodity. In the political aspect, seeing data sovereignty is a fundamental foundation in realizing state sovereignty in cyberspace. A country's data sovereignty is faced with the position of the state with the private sector in a global context. Cybersecurity systems and data sovereignty are inseparable in achieving state sovereignty in cyberspace. The main role of the state is to realize protection and maintain data security in national cyberspace. In 2017, the Government established the National Cyber and Crypto Agency (BSSN) which is a transformation of the National Crypto Agency which was combined with several other government agency work units related to cybersecurity. The presence of BSSN provides a very strategic key role in maintaining state sovereignty in cyberspace. This is in line with global challenges where cyber attacks and data leaks are increasingly rampant in Indonesia. For this reason, this study will explain the strategic role of BSSN in maintaining data sovereignty in order to realize state sovereignty in cyberspace. The author uses state theory and the concept of data sovereignty in analyzing this. The author uses qualitative methods to collect data through various literature studies, such as: books, journal articles, and other reference sources. The results of the study show that BSSN is a representation of the state's presence in maintaining the sovereignty of national cyberspace. This can be seen from the increase in Indonesia's cybersecurity index on a global scale which reflects an increase in national cybersecurity capabilities.

Keyword: Data Sovereignty, Cyber Security, State Sovereignty, Cyberspace.

INTRODUCTION

The development of data sovereignty in Indonesia is very important along with the advancement of global information technology that affects various aspects of national and state life. Data has strategic value and reflects state sovereignty, because data in a country can be used to support national development and people's welfare. Data sovereignty is also a manifestation of the state's existence in the digital or cyber realm. To achieve data sovereignty, effective data integration and management are needed, supported by a reliable data security system. In this case, a comprehensive national cybersecurity policy is needed. The presence of this policy will strengthen data sovereignty amidst the global dynamics that continue to develop due to advances in information technology. An optimal cybersecurity policy is very important in responding to increasingly complex global challenges. This policy will support the formation of an integrated and secure national data system, as well as increase the country's competitiveness in the global economy and politics. The core of this policy is the establishment of an institution that plays a central role in maintaining cybersecurity in order to realize digital data sovereignty in Indonesia.

In 2021, data leak incidents have become more frequent. These leaks involve state-owned data in various government agencies as well as personal data of citizens stored in government agencies and the private sector. According to a report by the National Cyber and Crypto Agency (BSSN), there were around 1.6 billion cyber attacks throughout the year. Meanwhile, data from the cybersecurity agency The Record, Insikt Group, quoted by CNN Indonesia (2021) revealed that hackers from China managed to penetrate the cybersecurity systems (firewalls) of around 10 Indonesian government agencies, including the State Intelligence Agency (BIN). This attack is suspected to have been carried out by Mustang Panda, a hacker from China who is known to often target countries in Southeast Asia. The rampant data leaks in various Indonesian agencies are due to the lack of integration of national cybersecurity policies between ministries and related institutions. This is exacerbated by the absence of a central institution that has full authority to coordinate and secure national data sovereignty as a whole.

Various incidents of data leaks and cyber attacks have hit a number of agencies in Indonesia, both from the government and private sectors. In fact, personal data belonging to Indonesian citizens has been traded on various illegal sites for the personal gain of irresponsible parties. This condition certainly harms the owners of the data significantly. In addition, the national digital ecosystem is not yet fully protected by a reliable cyber security system, so it has the potential to hinder the growth and activities of society in the digital realm. Several cases of data leaks and cyber attacks that have occurred in recent years in Indonesia can be identified through the following table:

Table of Data Leakage Incidents and Cyber Attacks in Indonesia

No.	Agency Name	Year	Type of Data Breach
1.	Lazada	2020	Leak of 1.1 million data
2.	Tokopedia	2020	91 million user data leaked
3.	KPU	2020	There are claims from hackers that 2.3 million Indonesian citizens' data from the KPU has been hacked.
4.	BPJS Kesehatan	2021	Around 270 million Indonesian Citizen Data in BPJS Kesehatan Sold in Raid Forums
5.	BRI Life	2021	Alleged two million BRI Life customer data sold for Rp 101.6 million ($7,000)
6.	BIN	2021	Alleged hacking of BIN website
7.	Ministry of Communication and Information	2022	PSE site hacking
8.	Ministry of Defense	2023	Alleged hacking of the site by hackers
9.	Ministry Of Home Affair	2023	Alleged data leak of 337 million population and civil registration data
10.	KPU	2024	The Permanent Voter List data held by the KPU is suspected of having been leaked

Source: Compiled from various sources

The rapid development of technology has brought about significant transformations to the structure of national and state life. In recent years, issues regarding data sovereignty and cybersecurity have experienced an escalation of urgency, which were previously not seen as crucial aspects. Along with global dynamics, data sovereignty is now a reflection of a country's sovereignty in the digital realm or cyberspace. Data sovereignty refers to the principle that data must be subject to the regulations and legal systems of the country where the data is physically stored (Hummel et al., 2021). In an effort to build a strong and effective national cybersecurity policy framework, the existence of a state institution that has the authority and capacity to represent state sovereignty in cyberspace is needed. This institution is responsible for maintaining and protecting data, which has now become a strategic commodity with high economic value. Thus, the formation of a main body that acts as the main driver and director in the formulation and implementation of national cybersecurity policies is an urgent need.

The National Cyber and Crypto Agency (BSSN) was established by President Joko Widodo in 2017 as a result of the transformation of the National Crypto Agency (Lemsaneg), a government institution previously responsible for cryptography or information security. This transformation was accompanied by increased authority, budget allocation, and expansion of the organizational structure from Lemsaneg to BSSN. The establishment of BSSN reflects the active role of the state in ensuring national cybersecurity, with a strategic function in strengthening coordination and collaboration between ministries and institutions that are stakeholders in the cyber sector. The presence of the state in this cyberspace is expected to strengthen data sovereignty while creating a safe cyber environment.

Revitalization of the National Cyber and Crypto Agency of the Republic of Indonesia (BSSN-RI) is a crucial aspect in realizing a holistic national cybersecurity policy. The change in status of the National Crypto Agency (Lemsaneg) to BSSN marks the expansion of the mandate and responsibility of this institution in maintaining the data sovereignty of the Unitary State of the Republic of Indonesia (NKRI). The expansion of the organizational structure of BSSN also has an impact on increasing authority and budget needs to support the implementation of its main functions and duties. The presence of BSSN is a new milestone in the development of national cybersecurity in maintaining state sovereignty in cyberspace. The establishment of BSSN illustrates its strategic role in presenting the state to maintain and realize data sovereignty.

METHOD

This research was conducted with a descriptive analysis approach. The methodology used is qualitative in order to produce in-depth and systematic case study research. Qualitative research according to Yusuf (2017) explains that a qualitative researcher tries to explore the meaning and understand the meaning of the phenomena that occur by directly or indirectly being involved in the research object. Qualitative methods are research that specializes in producing meaning, concepts and others including a description of a natural and comprehensive event to be explained narratively. Qualitative research is a process of obtaining data, analyzing and interpreting it comprehensively so that a clear understanding of a problem is produced.

The author chose to use a qualitative approach because this study will describe, explain and analyze the strategic role of BSSN-RI which describes the presence of the state in national cybersecurity policy. The context of cybersecurity and data sovereignty is very fundamental in the development of current global challenges. The author uses the theory of the state and the concept of data sovereignty in analyzing this. The type of data contained in this study is a literature study. Primary data collection techniques are obtained through books and relevant journal articles, to various media both online and print, as well as other sources of information that will be used to support this research. Literature Study is used by the author in order to be able to analyze the data that has been obtained comprehensively.

RESULTS AND DISCUSSION

The implementation of national cyber defense until 2012 was still not integrated and tended to be sectoral, where each government agency prioritized its own capabilities and interests. Both government agencies and the private sector carried out cyber defense efforts separately. Several government agencies involved include the National Cryptography Agency (Lemsaneg), the Ministry of Communication and Information (Kemenkominfo), the State Intelligence Agency (BIN), the Indonesian National Armed Forces (TNI), and the Ministry of Defense. On the other hand, educational institutions and communities such as the University of Indonesia, Gadjah Mada University, the Sepuluh Nopember Institute of Technology, the Bandung Institute of Technology, and the Indonesian Computer Emergency Response Team (ID-CERT) also contributed. Meanwhile, from the business sector, industry players such as banking, gas and oil, telecommunications, and various other business entities (Fitriati, 2018).

According to Harold J. Laski as quoted by Syaiful Bakhri (2018), a country is understood as a community that is united because of the existence of an authority that has coercive power and formal legitimacy, and has a higher position than other elements in society. Society itself is a group of individuals who live together with goals that they want to achieve collectively. A society can be called a country if the rules of living together are determined by an authority that is coercive and binding. The National Cyber and Crypto Agency (BSSN), which is a form of transformation of the National Crypto Agency (Lemsaneg), represents the strategic role of the state in ensuring cyber security and maintaining national data sovereignty.

The National Cyber and Crypto Agency (BSSN) was formed through the merger of several previously existing government institutions, such as the National Crypto Agency (Lemsaneg), the Directorate of Information Security of the Ministry of Communication and Information, and the Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII). This merger was stipulated through Presidential Regulation (Perpres) Number 53 of 2017. Then, the regulation was refined with the issuance of Presidential Regulation Number 28 of 2021, which aims to reorganize the organizational structure of BSSN in order to strengthen Indonesia's cyber sovereignty. Details regarding changes to the structure and working mechanisms of BSSN are further regulated in BSSN Regulation Number 6 of 2021 (BSSN RI, 2023). The formation of BSSN reflects that the state has been present to guard the national cyberspace.

A strong and authoritative organization is needed to maintain the sovereignty of the country in cyberspace. This organization must be formed with a grand design and a clear vision and mission to protect national cyber sovereignty. The existence of this organization is important to ward off various cyber threats, maintain national information resources, protect strategic data and information, secure vital information and communication technology infrastructure, and strengthen cooperation at the national and international levels in managing cyberspace. In addition, this organization also needs to aim to strengthen national cyber defense capabilities. Other targets include building synergy in cyber defense policies, forming effective cyber security institutions and governance, creating a resilient cyber defense system, improving cyber security for the government and society, and encouraging the development of national cyber research (Fitriati, 2018).

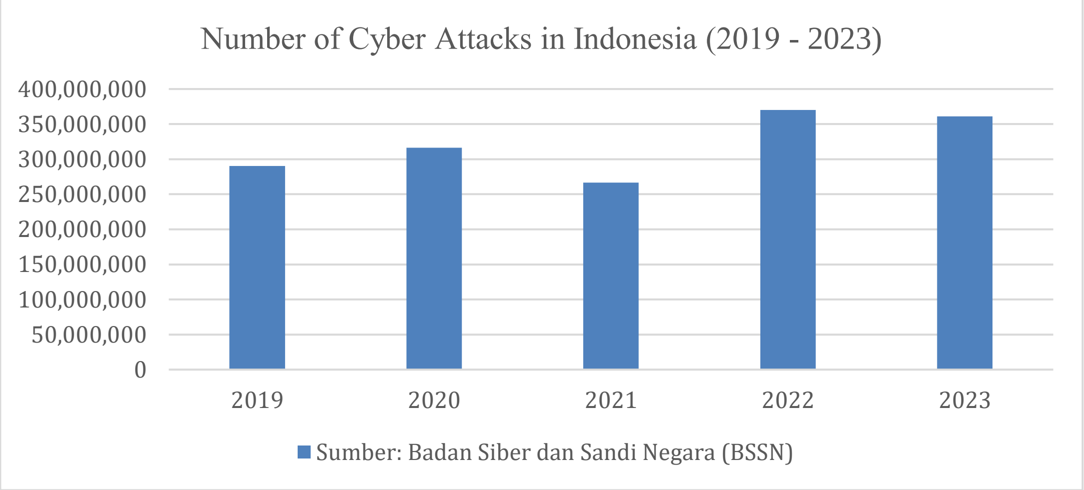
Polatin-Reuben and Wright in Baezner and Robin (2018) define data sovereignty as a state's effort to control information generated within or across its borders. This definition includes a series of strategic policies and actions aimed at gaining full authority over the data. A key element in this concept is the state's desire to ensure that data remains within national jurisdiction to prevent access or surveillance by foreign parties. Furthermore, Polatin-Reuben and Wright (2014) in Baezner and Robin (2018) place data sovereignty as an important component in a broader framework, namely cyber sovereignty.

A country's data sovereignty is highly dependent on the location of the data center, whether it is within its territory or abroad. When the data center is stored outside the national territory, and the country does not have adequate cyber diplomacy capabilities, the risk to data security increases. For example, if companies such as Instagram, Facebook, WhatsApp, Twitter, and Google have not placed their data centers within the country, then the country in question will have difficulty enforcing laws related to the protection of its citizens' data. This is a crucial issue in the context of data sovereignty.

In many developing countries, people are the main consumers of these technology services, but companies that own the services often have not built data centers in the country. As a result, developing countries are often helpless when data misuse occurs. Indonesia also faces a similar situation, where most global technology companies have not placed their data centers in Indonesia, and many do not have permanent representative offices. From a political economy perspective, this can be a major obstacle for Indonesia in dealing with the data sovereignty crisis.

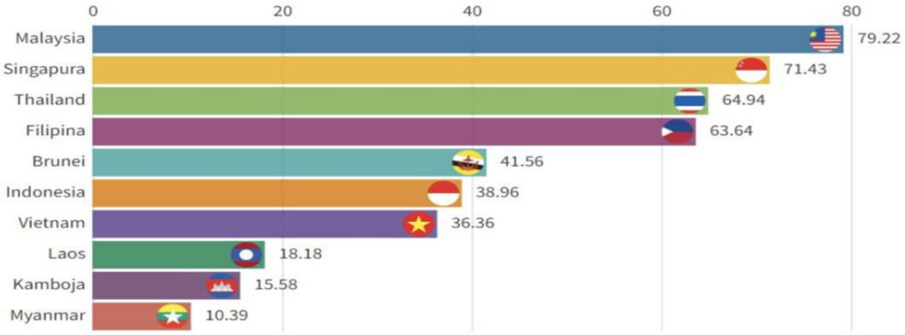
Sudibyo (2019) stated that state involvement in the global digital landscape has positive and negative impacts. Companies such as Facebook, Google, and Amazon not only promote democratic values, but also pursue economic interests by commodifying data. Social media applications are not provided for free, because they are actually business products that aim to make a profit. This platform stores internet user behavior data to build more sophisticated algorithms and artificial intelligence, as well as more targeted digital advertising. This data has become a primary commodity that generates huge profits, even though users do not know how and to whom their data is sold. This phenomenon is also reflected in the increasing cyber attacks in Indonesia. This development must be responded to immediately so as not to harm the nation. Community activities that are now shifting to the digital realm require regulations and institutions that can guarantee national cybersecurity. The transformation of Lemsaneg into BSSN is expected to be a strategic step for the state in maintaining cyberspace, but its implementation still faces obstacles, including sectoral egos and the absence of special cybersecurity laws. To clarify the conditions related to cybersecurity, here is the cyberattack data from 2019 to 2023 released by BSSN:

Table of Number of Cyber Attacks in Indonesia from 2019 to 2023



The COVID-19 pandemic has had various impacts, one of which is a decline in Gross Domestic Product (GDP) in Indonesia. However, in the midst of these conditions, Indonesia's digital economic growth actually experienced a significant increase of 11% in 2020, with a value of around 44 billion US dollars. Indonesia also has a rapidly growing digital ecosystem, supported by around 2,000 startups that are actively running business activities, which has a major impact on the demand for cloud computing services domestically. Of the 13 unicorns in the ASEAN region, five of them are from Indonesia, and they are the main users of cloud services in their business operations. These facts show that Indonesia has a strategic position in the digital economy market, both nationally and globally. Therefore, a strong institution is needed to ensure data sovereignty, so that this great potential can be utilized optimally for the benefit of the Indonesian nation (Amiruddin et al., 2023).

Since the establishment of BSSN, Indonesia has experienced an increase in the cybersecurity index. This shows that the presence of BSSN has a strategic role in representing the country in cyberspace. Based on the 2022 National Cyber Security Index (NCSI) report, Indonesia obtained a cybersecurity score of 38.96 out of a total of 100 points. This score places Indonesia in the third lowest position among the G20 member countries. Globally, Indonesia is ranked 83rd out of 160 countries listed in the report. The data can be seen in the following diagram:



Source: Breached.to in (Daeng et al.,2023)

Meanwhile, in 2023, the Indonesian Cyber Security Index increased its score quite significantly. This shows that there is a change towards a more positive direction in national cyber security capabilities. This shows that the establishment of the National Cyber and Crypto Agency has consistently shown quite significant increases in cyber security scores in Indonesia, which represents an increasingly capable national cyber security system

NCSI's 2023 Southeast Asia Cybersecurity Index

No.	Negara	Skor
1.	Malaysia	79,22
2.	Singapura	71,43
3.	Thailand	69,94
4.	Filipina	63,64
5.	Indonesia	63,64
6.	Brunei Darussalam	41,56
7.	Vietnam	36,36
8.	Kamboja	23,38
9.	Laos	18,18
10.	Myanmar	10,39

Source: Databoks.Katadata

According to Ristianto in Cloramidine, and Baharuddin (2023), along with the increasing number of internet users in Indonesia, the number of cyber attacks has also increased. This increase in attacks also reflects the extent to which the government is serious about handling cybersecurity issues. This commitment is reflected in the improvement in Indonesia's score in the Global Cybersecurity Index (GCI) which continues to show a positive trend every year. Former Head of the National Cyber and Crypto Agency (BSSN), Djoko Setiadi, revealed that according to GCI data released by the International Telecommunication Union (ITU), Indonesia managed to rise to 41st place out of 175 countries in 2018, and was ranked 9th in the Asia-Pacific region. Furthermore, according to ITU data in Cloramidine, and Baharuddin (2023), in

2020, Indonesia's position increased to 24th place out of 194 countries globally, and was ranked 6th in the Asia-Pacific with a score of 94.88.

In formulating cybersecurity policies and realizing data sovereignty, Indonesia can learn from countries that are more advanced in this regard, such as Estonia. According to Robinson and Hardy in Romaniuk and Manjikian (2021), Estonia experienced a major cyberattack in April to May 2007, known as the "Bronze Night" incident. This incident began with the removal of a World War II-era Soviet monument from the center of Tallinn, which sparked strong protests from the Russian-speaking community. The monument has different historical meanings for Estonian nationalists and citizens of Russian descent, so its removal sparked tensions. As a result, Estonia experienced a DDoS (Distributed Denial of Service) attack that paralyzed various vital state services, including government websites, banks, media, and political parties. Although the main services were restored within a day, the attack continued for almost three weeks, from April 27 to May 18, 2007. As a result of this incident, accusations arose that Russia was involved, which worsened diplomatic relations between the two countries. However, the involvement of the Russian government is difficult to prove with certainty.

The attack was later seen by some Estonians as a wake-up call to the importance of cybersecurity. The incident prompted a major shift in national digital security policy. Estonia responded by developing a National Cybersecurity Strategy, which was unveiled in May 2008, and has become one of the main references in the development of modern cybersecurity strategies today. The strategy places cybersecurity as a critical element on a par with traditional national defense interests. On a global scale, Estonia’s approach to cybersecurity is particularly interesting. Estonia has a Data Embassy in Luxembourg, which, according to Robinson and Hardy in Romaniuk and Manjikian (2021), allows the country to store backups of critical databases and information systems outside its borders. This allows Estonia to continue operating effectively even in the event of a crisis or major disruption to its digital infrastructure. In October 2018, Estonia adopted its third National Cybersecurity Strategy for the period 2019–2022. This strategy did not involve a major overhaul of the organization, but rather continued the approach of the previous strategy. However, during this period the National Cybersecurity Center was established. The strategy aims to ensure the resilience of vital state functions, such as critical infrastructure and elements of Estonia’s digital society as a whole. Initiatives include the implementation of the “no legacy” principle, a policy of the Digital Agenda 2020 that requires public sector ICT systems to be updated every 13 years to remain modern and efficient. The strategy also continues the development of the Data Embassy and prepares for the adoption of next-generation technologies.

At the EU level, Estonia has aligned its national policies with the NIS Directive and the GDPR Regulation which came into force in May 2018. According to Robinson and Hardy in Romaniuk and Manjikian (2021) this alignment was realized through the enactment of Estonia's first Cybersecurity Act and the revision of the Personal Data Protection Act in the same year. In the field of education, Estonia has also made efforts to strengthen cyber defense, with TalTech (Tallinn University of Technology) becoming a center of excellence in digital forensics and cybersecurity. Data protection oversight is carried out by the Data Protection Inspectorate. Estonia also plays an important role as the host of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and is active in global cyber exercises such as Locked Shields. This exercise is now open to non-NATO countries such as Finland, New Zealand, and South Korea. With a fourth strategy planned to start in 2023, Estonia is expected to continue to be a global leader in cybersecurity issues.

The establishment of BSSN is the right direction so that the country can have an agency that has a strategic role as a central institution in the field of national cybersecurity. This is in accordance with what has been developed by other countries that have long developed and optimized their respective cybersecurity sectors. In the future, of course, there will be more challenges to be faced considering the increasing number of cyber attacks with various types that are very dynamic. The development of the cybersecurity sector as carried out in Estonia can be one of the benchmarks for Indonesia for the development of BSSN in the future.

CONCLUSION

The establishment of the National Cyber and Crypto Agency (BSSN) of the Republic of Indonesia illustrates the presence of the state in guarding cyberspace. This shows that the state is carrying out its role in protecting state sovereignty in cyberspace. This description is in accordance with the view of the state theory which explains that the state must be present to provide protection. In today's technological developments, the protection implemented is not only in physical space but also encompasses cyberspace.

Sovereignty is a state's action to control information obtained within or across its borders. The context of this sovereignty includes policies and strategic actions aimed at gaining full authority over the data. The strategic role of BSSN as a representation of the state in maintaining data sovereignty is very fundamental. This can be seen from the increasing Indonesian cybersecurity index based on the results of the NCIS report. Based on this, it can be said that Indonesia's cybersecurity capabilities needed to maintain state sovereignty in cyberspace have increased. In the future development of BSSN, Indonesia can also follow the example of various other countries that have already developed their cybersecurity sectors such as Estonia. BSSN is a central agency where its strategic role in the field of cybersecurity reflects state sovereignty

REFERENCE

Amiruddin, et al. (2023). Tinjauan Strategis Keamanan Siber di Indonesia: Teknologi Cloud dan Tata Kelola Data. Politeknik Siber dan Sandi Negara - Universitas Indonesia: Jakarta. A Muri Yusuf. 2017. Metode Penelitian: Kuantitatif, Kualitatif, Dan Penelitian Gabungan. Jakarta: Kencana.

Bakhri, Syaiful. (2018). Ilmu Negara: Dalam Pergumulan Filsafat, Sejarah dan Negara Hukum, Depok: PT. Raja Grafindo Persada.

Baezner, Marie & Patrice Robin. (2018). Cyber Sovereignty and Data Sovereignty. CSS Cyberdefense Trend Analyses Version 2, Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich.

BSSN RI. (2019). Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber.

BSSN RI. (2023). Lanskap Keamanan Siber Indonesia 2023.

Cloramidine, Feline, & Muhammad Badaruddin. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). Jurnal Sosial dan Humaniora Volume 8, Nomor 1, Tahun 2023. Universitas Nasional. Jakarta.

CNN Indonesia, Jaringan BIN dan Kementerian Dilaporkan Dibobol Hacker China,

https://www.cnnindonesia.com/nasional/20210912112723-20-693110/jaringan-bin-dan-kementerian-dilaporkan-dibobol-hacker-china

Daeng, Yusuf, et al. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. INNOVATIVE: Journal Of Social Science Research Volume 3 Nomor 6.

Databoks.katadata.co.id, Indeks Keamanan Siber Indonesia Tertinggi ke-5 di ASEAN 2023.

https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/5bf8dbfb3998ee8/indeks-keamanan-siber-indonesia-tertinggi-ke-5-di-asean-2023

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

Hummel, Patrik, et al. (2021). Data Sovereignty: A review. Big Data & Society. January-June: 1–17. Sage Publication Ltd.

Sudibyo, Agus. (2019). Jagat Digital: Pembebasan dan Penguasaan. KPG: Jakarta.

Romaniuk, Scott N & Mary Manjikian (ed). (2021). Routledge Companian To Global Cyber Security Strategy. Routledge: New York.