Eduvest – Journal of Universal Studies
Volume 5 Number 5, May, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

THE IMPACT OF CYBER ATTACKS ON NATIONAL DATA CENTERS ON NATIONAL RESILIENCE: A CASE STUDY OF SOEKARNO HATTA AIRPORT IMMIGRATION CHECKPOINTS

Annisa Nuril Ikhtiram*, Ibnu Hamad
Universitas Indonesia
Email: annisanuriltiram7@gmail.com, ihamad966@gmail.com

ABSTRACT

This study analyzes the impact of cyber attacks on the National Data Center (PDN) on national resilience, with a case study of the Immigration Checkpoint at Soekarno Hatta Airport. Cyber attacks on the PDN, which paralyzed the immigration system, exposed the vulnerabilities of digital infrastructure that is crucial to the continuity of public services. This study examines how disruptions to immigration services impact mobility, the economy, and the country's image. The economic impact is analyzed through potential losses due to flight delays, decreased tourism, and disruption to the supply chain. The social aspect is examined through the psychological impact on society due to uncertainty and discomfort. The weaknesses of the National Data Center (PDN) are not only understood as technical problems that disrupt administrative services, but also as issues that have a direct impact on the vital function of the Immigration Checkpoint (TPI). TPI has a strategic role in managing the flow of population migration, both Indonesian Citizens (WNI) and Foreign Citizens (WNA), who leave and enter through the country's border areas. Furthermore, this study explores how the attack affects public trust in the government's ability to protect vital data and infrastructure. The analysis of national resilience focuses on how cyber attacks can weaken the stability of the state and damage the government's ability to carry out its functions. This study emphasizes the need for investment in strengthening cybersecurity systems and increasing public awareness to minimize similar impacts in the future. These findings are expected to provide insight for policy makers in strengthening national resilience in the digital era.

KEYWORDS Cybercrime, Cyber Security, National Data Center, National Resilience, Population Migration

INTRODUCTION

Cybersecurity, or cyber security, is a practice that aims to protect computer systems, networks, and data from various threats or illegal access. This term comes from two words in English, namely "cyber," which refers to cyberspace (internet),

How to cite: Annisa Nuril Ikhtiram, Ibnu Hamad (2025). The Impact Of Cyber Attacks On National Data Centers On National Resilience: A Case Study Of Soekarno Hatta Airport Immigration Checkpoints. Journal Eduvest. *5* (5): 5583-5595.
E-ISSN: 2775-3727
Published by: https://greenpublisher.id/

and "security," which means security. Cybersecurity encompasses various efforts to maintain the integrity, confidentiality, and availability of information in the digital environment. Cybersecurity in the digital age has become an issue, especially in national security. With more and more data and information stored online, the risk of cyberattacks increases significantly. These attacks not only threaten individuals or companies, but can also undermine the stability and security of a country.

In the digital age, cybercrime, or cybercrime, has evolved into a complex threat. Attacks such as malware, ransomware, and phishing can damage information systems, steal personal data, and disrupt economic activities. In Indonesia, for example, the State Cyber and Cryptography Agency (BSSN) reported that in 2021 there were more than 1.6 billion cyberattacks. This figure shows how vulnerable our digital infrastructure is to external threats. Cybersecurity serves as a shield for data and information systems. Without adequate protections, sensitive data can fall into the wrong hands, potentially causing financial and reputational losses for individuals and organizations alike. Nationally, cyberattacks can disrupt public services and critical infrastructure, putting the safety of the community at risk.

Cyber threats to national security encompass a wide range of aspects, from data theft to attacks on critical infrastructure. For example, a DDoS (Distributed Denial of Service) attack can make government or corporate services unavailable to legitimate users. In addition, attacks on government systems can result in problems with sensitive information that have the potential to endanger national security. Changes in the global environment also contribute to the complexity of these threats. Traditional threats focused on military power have now shifted to non-traditional threats such as cyber warfare. Countries must adapt quickly to protect themselves from increasingly sophisticated cyberattacks.

The impact of cyberattacks is vast and can be felt in various sectors. In the economic sphere, these attacks can cause significant financial losses for companies and individuals. Ransomware attacks, for example, encrypt important data and demand a ransom to return it. This is not only financially detrimental but can also damage the company's reputation in the eyes of customers. From a social perspective, cyberattacks can cause public distrust of digital technology and services. If people feel that their data is not secure, they may be reluctant to use online services that are essential to their daily lives. This can hinder the development of the digital economy which is urgently needed in this modern era.

To meet these challenges, collaboration between the government, the private sector, and society is needed. The Indonesian government has taken steps by implementing regulations such as the Electronic Transaction Information Law (UU ITE) to protect data and information systems from digital attacks. In addition, education about cybersecurity needs to be improved so that people are more aware of potential threats and how to protect themselves. The use of security technologies such as firewalls and antiviruses is also crucial in protecting the system from malware attacks and data theft. Additionally, continuous monitoring of network activity can help detect anomalies or potential attacks before they cause greater damage.

A map is supposed to provide flexibility so as to depict "many roads to Rome". From the map of the future of cybersecurity, there are many signs and boxes that must be watched out for while traveling. However, as a trip should be well structured, the initial and end destinations and which priorities should be done first. Whether the 20 recommendations map seeks to show the actual order of priorities and according to reality must be checked with the conditions and realities faced. However, we think that the 20 recommendations represent conditions that may exist and occur in Indonesia. The second problem is related to bureaucratic culture, that a Roadmap can be used as a reference if it has been approved by the parties involved in the ecosystem and ratified by the State as the authority holder .

The cyberattack that occurred at Indonesia's National Data Center (PDN), especially affecting immigration services at Soekarno-Hatta Airport, is an incident that reflects the vulnerability of the country's cybersecurity system. This incident began on June 17, 2024, when the State Cyber and Cryptography Agency (BSSN) detected an attempt to disable Windows Defender's security features, which allow malware, including ransomware, to access the system. The ransomware used in this attack is known as Brain Cipher, which is a variant of the Lockbit 3.0 ransomware.

The impact of these attacks was significant, causing disruptions to various public services, especially immigration services. On June 20, 2024, a long queue occurred at Soekarno-Hatta International Airport because the immigration system had to operate manually due to a malfunction in the PDN system. The Director General of Immigration, Silmy Karim, stated that after 12 hours of disruption, his party decided to move the data center in order to restore services. These attacks are not isolated incidents; Indonesia has been the target of cyberattacks on a regular basis. The BSSN report shows that in 2021 alone, there were more than 1.6 billion traffic anomalies or cyberattacks detected throughout Indonesia. This shows that the threat to cybersecurity in Indonesia is very real and sustainable. Cybersecurity experts state that weaknesses in government IT infrastructure and lack of effective backup systems have contributed to this vulnerability.

The weakness of the National Data Center (PDN) has a significant impact on migration flows at Immigration Checkpoints (TPI), both for incoming and outgoing passengers, including Indonesian citizens and foreigners. When the PDN is disrupted, the immigration check system, which usually runs automatically through autogates and digital applications, becomes paralyzed. As a result, the entire inspection process must be carried out manually by officers. The switch to manual systems led to long queues and passenger build-up in immigration areas, as happened at Soekarno-Hatta Airport and other airports and ports in Indonesia. Passengers, both departing and newly arrived, will have to wait longer for immigration document checks. This slows down the flow of people in and out, disrupts flight schedules, and increases the risk of travel delays massively.

In addition, the disruption to the PDN also affects other services related to immigration data, such as passport validation for the creation of NPWP for foreign nationals. Processes that can usually be done online are hampered because immigration data cannot be accessed in real time. This condition shows that the weak PDN not only has an impact on the technical aspects of inspections at TPI,

but also on cross-agency administrative services that require digital verification of immigration data.

The absence of strict regulations also has implications for public trust in digital systems. People tend to feel worried about the security of their personal data when there is no clear legal framework to protect the information. Public trust is a key element in the digital ecosystem; Without trust, public participation in digital services will decrease. In addition, rapid technological developments are often more advanced than existing regulations. Many companies and organizations have not fully understood or implemented best practices in cybersecurity, especially when it comes to complying with existing regulations. This creates a loophole where cyberattacks can occur more easily. For example, ransomware attacks and data theft can occur due to a lack of understanding of how to effectively protect information systems.

Current regulations also often do not cover all the important aspects of cybersecurity. For example, although the PDP Act provides some guidelines on personal data protection, many organizations still struggle to meet the requirements set. A more holistic and integrated approach is needed to address this issue. Cooperation between the public and private sectors is also crucial to creating effective and enforceable policies. In an international perspective, many countries have developed a more comprehensive legal framework to deal with cyber threats. Indonesia needs to learn from these best practices and adapt to local needs. The establishment of stricter regulations will not only improve national security but will also build public trust in the country's digital infrastructure. The absence of strict regulations in the cybersecurity system in Indonesia creates loopholes that have the potential to be exploited by malicious parties. To overcome these challenges, collaborative efforts from all stakeholders are needed to formulate more comprehensive and effective laws in protecting the country's data and digital infrastructure .

The purpose of this study is to analyze the impact of cyber attacks on the National Data Center (PDN) on national resilience, with a focus on the case study on the Immigration Checkpoint at Soekarno Hatta Airport. The study aims to identify vulnerabilities in cybersecurity systems that affect public services, measure the economic and social impacts of immigration service disruptions, and evaluate the implications for public trust and state stability. In addition, this research aims to provide strategic recommendations to strengthen the national cybersecurity system and increase resilience to future digital threats.

RESEARCH METHOD

Qualitative research with a descriptive-analytical approach is a method used to understand social phenomena or human behavior through in-depth data collection and systematic analysis. This approach focuses on a detailed description of the context, meaning, and experience of the research subject. In this study, the researcher seeks to explore the perspectives of individuals or groups through observations, and documents, so as to uncover the patterns and themes that emerge from the collected data. The analysis is carried out inductively, where the researcher interprets the data to find deeper relationships or meanings. The results of this

research are often presented in the form of rich narratives, providing insight into how individuals perceive and interact with the world around them.

In research on cyber attacks on the National Data Center and its impact on national resilience, some of the data sources that can be used include official reports from the Statistics and analysis of cyberattacks in Indonesia generally provided by the State Cyber and Cryptography Agency (BSSN) and the Ministry of Communication and Information Technology (Kemenkominfo), which routinely release reports related to incidents and handling of attacks, including the PDN ransomware incident in June 2024. In addition, the official report from the Directorate General of Immigration of Soekarno-Hatta Airport has also explained in detail the chronology of the disruption, the impact on long queues, the delay in inspections, and the restoration of immigration services after the attack. Regarding cybersecurity and mitigation measures are also very relevant. News articles from national media such as Kompas, Detik, and Tempo can provide context and details about specific incidents that occurred at Soekarno-Hatta Airport. Academic research on cybersecurity, published in scientific journals, can also provide in-depth insights into cyberattack trends and effective defense strategies.

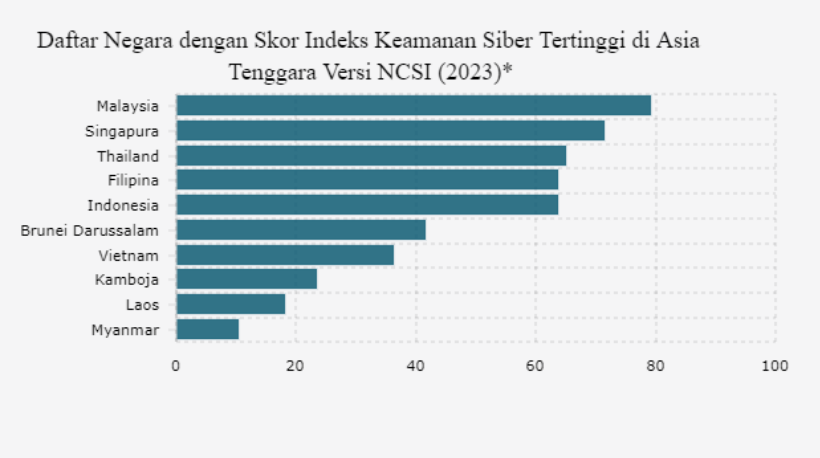
The data collection technique in this study uses a qualitative approach by combining observation and documentation studies. Observations were carried out directly at the Soekarno-Hatta Airport Immigration Checkpoint to understand the real impact of cyber attacks on the immigration process and public services. In addition, the documentation study was carried out by examining official reports, news, and relevant policy documents to complete the primary data. The combination of these three techniques aims to obtain a comprehensive picture, strengthen the validity of the data, and support an in-depth analysis of the phenomenon being studied.

Data analysis in this study uses a descriptive-analytical approach to understand cyber attacks on National Data Centers (PDN) and their impact on national resilience. Data from the State Cyber and Cryptography Agency (BSSN) provides statistics on the frequency, type, and pattern of attacks, specifically the Brain Cipher ransomware incident that infected PDN and disrupted public services since June 2024. Documents from the Ministry of Communication and Information Technology (Kemenkominfo) are analyzed to assess the government's cybersecurity policies and mitigation strategies, which are currently being strengthened through data protection design and periodic simulations. Information from national media such as Kompas, Detik, and Tempo provides context for the incident and its impact on critical infrastructure, such as Soekarno-Hatta Airport. Scientific journals add an academic perspective to understand the evolving trends and patterns of cyber threats. Inductive analysis identifies attack patterns that show a broad impact not only on information security, but also on economic and social stability, thus demanding more comprehensive and integrated mitigation measures to maintain national resilience.

RESULT AND DISCUSSION

Cybersecurity Analysis in Indonesia

Indonesia has developed a number of regulations related to cybersecurity, including the Information and Electronic Transactions Act (UU ITE) which was first passed in 2008 and revised in 2016 and the Personal Data Protection Law. The ITE Law and the PDP Law provide a legal framework for electronic transactions and data protection, but many consider them to be weak in terms of personal data protection. The State Cyber and Cryptography Agency (BSSN) was formed to address cybersecurity challenges in Indonesia. BSSN has a responsibility in developing a national cybersecurity strategy. However, despite the efforts of BSSN, many reports indicate that the budget for cybersecurity is still limited, affecting the agency's ability to carry out its duties effectively. For example, a report from the National Cyber Security Index (2021) shows that Indonesia ranks 5th out of 10 ASEAN countries with relatively low index scores, reflecting weaknesses in regulation and protection of essential services.



Gambar 1. Indeks Keamanan Siber Indonesia Tertinggi ke-5 di ASEAN 2023
Source: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/5bf8dbfb3998ee8/indeks-keamanan-siber-indonesia-tertinggi-ke-5-di-asean-2023*, 9 Januari 2025*

The image shows a list of countries in Southeast Asia with the highest Cybersecurity Index (NCSI) scores in 2023. The scale on the horizontal axis indicates the cybersecurity score, which ranges from 0 to 100. The countries are arranged in order based on highest to lowest scores. Malaysia ranks first with the highest score, close to 80, which shows that the country has an excellent cybersecurity system in the region. Singapore is in second place with a slightly lower score than Malaysia, but is still in the very high category. Thailand and the Philippines are in the next position with quite competitive scores, showing that they also have a solid cybersecurity system.

Indonesia ranks fifth, with a lower score than the previous four countries, but still significant compared to other countries in the region. Brunei Darussalam and Vietnam are next in the rankings, where their scores indicate a moderate level of cybersecurity. The last three countries on the list are Cambodia, Laos, and

Myanmar. These three countries have much lower scores than the rest of the countries, which suggests that they have a lot of room for improvement in their cybersecurity systems. This data is taken from the 2023 version of the NCSI (National Cyber Security Index), which assesses the extent to which a country is prepared to face cyber threats and protect their digital data. The index reflects a country's ability to protect its digital ecosystem, including infrastructure security, data protection, and response to cyber incidents.

One of the main gaps in data protection in Indonesia is the lack of integration between various existing regulations. Cybersecurity responsibilities are shared between several ministries and institutions, such as the Ministry of Communication and Information Technology (Kominfo) and the Coordinating Ministry for Political, Legal and Legal Affairs, but without clear coordination. This often results in overlapping tasks and confusion about who is in charge in certain situations. This ambiguity can slow down the response to cyber incidents. Additionally, many companies, especially small and medium-sized enterprises (SMEs), do not yet fully understand the importance of cybersecurity or have the resources to implement best practices in data protection. This can create vulnerabilities that can be exploited by cyberattackers. Ransomware attacks and data theft are becoming increasingly common, indicating that many organizations do not yet have adequate risk mitigation measures in place. Existing regulations also often do not cover all aspects of cybersecurity. For example, although the ITE Act provides some guidelines on personal data protection, many organizations struggle to meet those requirements due to a lack of practical guidance or operational standards. This leads to uncertainty about how to effectively protect data.

The absence of a comprehensive Cyber Security and Resilience Bill is also a problem. Without a clear legal framework to address cyber threats comprehensively, government efforts to strengthen cybersecurity will be hampered. The bill should cover aspects such as cyber incident management, collaboration between the public and private sectors, and human resource capacity building in the field of cybersecurity. In a global scope, many countries have developed a more comprehensive legal framework to deal with cyber threats. Indonesia needs to learn from these best practices and adapt to local needs. The establishment of stricter regulations will not only improve national security but also build public trust in the country's digital infrastructure[1].

CASE STUDY OF CYBERATTACK ON IMMIGRATION PLACES

The cyberattack that occurred on Indonesia's Temporary National Data Center (PDNS) in June 2024 is one of the most significant incidents in the country's cybersecurity history, which has had a wide impact on various sectors, especially public services at Soekarno-Hatta Airport. The attack began on June 17, 2024, when the State Cyber and Cryptography Agency (BSSN) detected suspicious activity that led to the disabling of Windows Defender security features. This allows LockBit

[1] Daeng, Yusuf, et al. "Analysis of the Application of Cyber Security Systems to Cybercrime in Indonesia." *Innovative: Journal Of Social Science Research* 3.6 (2023): 1135-1145.

3.0-type ransomware, known as Brain Cipher, to infiltrate systems and encrypt critical data belonging to various government agencies.

The ransomware demanded a ransom of $8 million to restore access to encrypted data. However, the Indonesian government refused to meet these demands. This decision reflects the government's commitment not to negotiate with cybercriminals, despite the high risk of data loss. As a result of this attack, immigration services at Soekarno-Hatta Airport experienced significant disruptions. The immigration system that normally operates automatically is forced to function manually, causing long queues and delays in the immigration screening process. This causes inconvenience to thousands of passengers who use the airport every day.

Migration control, especially the management of passenger flows at Immigration Checkpoints (TPI), is one of the national resiliences affected by various factors, including infrastructure and immigration policies. Migration control is not just an administrative procedure for immigration services, but an integral part of safeguarding state sovereignty and national security. The management of the inflow and exit of passengers, both Indonesian citizens and foreigners, must be carried out selectively and strictly to prevent the entry of illegal immigrants, misuse of documents, and potential security threats such as human trafficking and drug smuggling.

After the Covid-19 pandemic, strict border controls have become increasingly crucial in reducing the risk of disease spread and maintaining national stability. Robust migration infrastructure and reliable inspection systems support effective monitoring of population movements, so as to identify and control potential external threats. The selective policy implemented at the TPI aims to ensure that incoming foreigners bring benefits and do not endanger security and public order. Thus, migration control plays a direct role in maintaining national resilience through careful monitoring of migration flows, not just the implementation of immigration administrative procedures. Weaknesses in migration controls, such as weak technological systems or lack of synergy between border control agencies, can open up loopholes for the influx of illegal immigrants that have the potential to disrupt social stability and national security.

In an effort to restore services, the government took emergency measures by moving data centers and isolating connections between the affected PDNS in Surabaya and other data centers in Serpong and Batam. This step aims to prevent further spread of malware and protect sensitive data from possible leaks. Although recovery efforts were carried out quickly, the impact of this attack has been felt by many parties[2].

This incident shows that Indonesia is becoming an increasing target of cyber attacks. The BSSN report noted that in 2021 alone, there were more than 1.6 billion

[2] Ramadhani, Eka Hero, I. Ketut Agung Enriko, and Erika Lety Istikhomah Puspita Sari. "Strategic Study of Cybersecurity Management on Telematics Projects in Indonesia: A Case Study of National Data Center Leaks." *Indonesian Journal: Informatics and Communication Management* 6.1 (2025): 570-580.

traffic anomalies or cyberattacks detected throughout Indonesia. This indicates that the threat to cybersecurity in the country is very real and ongoing. Weaknesses in the government's information technology infrastructure as well as the lack of effective backup systems contribute to these vulnerabilities. After a few days after the attack, the hackers finally gave the decryption key to the government for free. However, not all data is successfully recovered, and a lot of important information remains lost or corrupted. This incident reveals how vulnerable the government's digital infrastructure is in the face of increasingly sophisticated cyberattacks.

In response to the incident, the government together with BSSN conducted a thorough evaluation of the national cybersecurity system. They are committed to improving security protocols and accelerating the implementation of a more comprehensive cybersecurity strategy. Mitigation measures include training for government employees on cybersecurity, strengthening IT infrastructure, and increasing international cooperation in sharing information on cyber threats. The cyberattack on the Temporary National Data Center is a reminder of the importance of national resilience in the face of cyber threats. This incident highlights the need for greater investment in security technology and awareness of the risks that exist in today's digital age. The Indonesian government must continue to adapt and strengthen its security systems in order to protect sensitive data and critical infrastructure from future threats[3].

The Impact of Cyberattacks on Immigration Checkpoints

Cyber attacks on National Data Centers (PDN) in Indonesia, especially those that occurred in June 2024, have a significant impact on national resilience, especially in the field of public services. The immigration checkpoint at Soekarno-Hatta Airport is one of the real examples of this impact. The ransomware attack known as "*Brain Chiper*" resulted in the encryption of critical data and a ransom demand of USD 8 million. This attack not only affects the PDN, but also causes disruptions to the more than 210 government agencies that depend on the system. One of the most visible impacts is the accumulation of passengers at Terminal 3 of Soekarno-Hatta Airport, where long queues occur due to disruptions in the immigration screening system. The inspection process that is usually carried out automatically is forced to be switched to the manual method, slowing down the entire process and causing inconvenience to passengers.

The Brain Cipher ransomware attack that occurred on PDNS 2 since June 20, 2024 specifically paralyzed services at the Immigration Checkpoint (TPI), especially at Soekarno-Hatta International Airport. As a result of this attack, immigration screening systems were inaccessible, including autogate services, visa applications, residence permits, and M-Passports, leading to long queues for international passengers and delays in the departure and arrival process. More than 280 government agencies were affected, including the Directorate General of Immigration, and more than 200 public services were disrupted. The government

[3] Al Ihsan, Rafli, and Binastya Anggara Sekti. "The Importance of Data Security in the Digital Era: Reflections on Hacker Attacks on Indonesia's National Data Center." *SISFOTEK Proceedings* 8.1 (2024): 7-11.

refused to pay a ransom of 8 million US dollars demanded by the perpetrators of the Brain Cipher ransomware, a variant of Lockbit 3.0. For several days, the immigration service at TPI was completely paralyzed until the system was successfully migrated to the AWS cloud on June 22-23, 2024. This disruption has a significant impact on international mobility and the smooth running of immigration services in Indonesia[4].

The Director General of Immigration, Silmy Karim, confirmed that this disruption made all immigration-related services, including visa applications and residence permits, inaccessible. In an effort to restore service, immigration immediately migrated data to *Amazon Web Services* (AWS) as an emergency solution. Within two days of the attack, some systems were back up and running, although a full recovery took longer to ensure all data and applications were functioning properly. From a cybersecurity perspective, this incident shows significant vulnerabilities in the government's IT infrastructure. Cybersecurity experts assessed that this attack was one of the most severe ever experienced by Indonesian government agencies, highlighting the lack of a robust defense system and adequate data backups. The Ministry of Communication and Informatics is currently designing a better data protection strategy to prevent similar incidents in the future.

From a national resilience perspective, this attack shows the vulnerability of Indonesia's digital infrastructure. Weaknesses in the cybersecurity system indicate that the country is still not fully prepared to face increasingly sophisticated cyber threats. Data leaks due to these attacks can be used by interested parties, including other countries, for detrimental purposes. This raises concerns about the potential for future "cyber wars," where sensitive data could be used to undermine national stability. The recovery process takes more than a day and indicates that the data backup is unavailable or inadequate. In an effort to address this problem, the Ministry of Communication and Information Technology (Kemenkominfo) plans to build more permanent and secure national data centers in several strategic locations.

National Cyber Infrastructure Readiness

The readiness of Indonesia's national cyber infrastructure to deal with cyber threats is increasingly a major concern, especially after a series of attacks that disrupted public services and critical infrastructure. The Indonesian government has taken strategic steps to strengthen cybersecurity through comprehensive regulations. One of the Presidential Regulation Number 53 of 2017, which establishes a national strategy for cyber security and establishes the State Cyber and Cryptography Agency (BSSN) as the main institution in cybersecurity management. Cyber infrastructure readiness also includes developing the capacity of human resources (HR) in the field of cybersecurity. Currently, Indonesia is still

[4] Budiyanto, Deny, and Muhammad Mabruri. "THE IMPORTANCE OF CYBERSECURITY IN THE DIGITAL AGE: A GLOBAL OVERVIEW AND CONDITIONS IN INDONESIA." *Proceedings of the National Seminar on Science and Technology "SainTek".* Vol. 2. No. 1. 2025.

facing a shortage of trained experts in dealing with increasingly complex cyber threats. The government seeks to improve the number and quality of human resources through relevant training and education. Cooperation with the private and international sectors is also part of this effort to strengthen national capabilities in the face of cyber attacks.

Public awareness about cybersecurity is also the main focus. Many individuals and organizations still do not understand the risks that exist, so socialization campaigns about cybersecurity are urgently needed. The government has launched various programs to raise public awareness on how to protect themselves from cyber threats. Rapid detection and response systems to cyberattacks are also an important component in national cyber infrastructure readiness. The government has established Indonesia's *Computer Emergency Response Team* (CERT) to identify and respond effectively to cyber incidents. With this system, it is hoped that it can minimize the impact of the attack that occurs.

However, challenges remain. Reports show that Indonesia is one of the largest targets of cyberattacks in Southeast Asia, with more than 1.2 billion threats detected in 2023. Despite progress in infrastructure readiness, only about 39% of organizations in Indonesia are considered ready to face modern cybersecurity risks. This figure shows that most companies are still in the nascent stage when it comes to protection against cyber threats. In order to improve the readiness of national cyber infrastructure, the Zero Trust approach is one of the proposed strategies. This approach emphasizes the need to verify the identity of each user and device before granting access to the system, thereby reducing the risk of attacks from inside and outside the network. The readiness of Indonesia's national cyber infrastructure still needs to be strengthened in various aspects, ranging from policies to public awareness. With the increasing complexity and frequency of cyberattacks, governments must continue to adapt and strengthen security systems to protect sensitive data and critical infrastructure from existing threats. Collaborative efforts between the government, the private sector, and the community are essential to create a secure and trusted digital ecosystem in Indonesia.

Cyber Attack Mitigation Policies and Strategies

Cyber attack mitigation policies and strategies aim to maintain the security of information and digital infrastructure in Indonesia. National and international cybersecurity policies, prevention and early detection strategies, and the role of international cooperation are three interrelated and crucial aspects. Indonesia's national cybersecurity policy has evolved rapidly in recent years, with various regulations designed to protect critical data and infrastructure. One of the main foundations is Presidential Regulation No. 47 of 2023 which regulates the National Cybersecurity Strategy and Cyber Crisis Management. This policy aims to improve the country's cyber capabilities in the face of evolving threats. Within this framework, the government also implements a zero trust approach, which emphasizes that no entity in the network is automatically trusted, so any access must be strictly verified. Other regulations that support this policy include Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection. These two laws provide a legal framework for the management of data and electronic transactions, as well as

establish the responsibility for electronic system operators to maintain data security. At the international level, Indonesia actively participates in global cybersecurity forums to share information and experiences related to cyber threats. This cooperation is important to adapt effective policies based on best practices from other countries.

Cyber attack prevention and early detection strategies in Indonesia involve a variety of proactive measures to identify potential threats before they can cause damage. One of the main approaches is to strengthen information technology infrastructure through the implementation of advanced security systems, such as firewalls, intrusion detection systems, and data encryption. The government has also established Cyber Incident Response Teams at the national and sectoral levels to respond quickly and effectively. In addition, training for human resources in the field of cybersecurity is the main focus. Increasing awareness of cyber risks among government employees and the private sector is essential to creating a strong security culture. The government also held a simulated cyber attack to test the readiness of the system in the face of real threats. Early detection is also supported by the use of analytics technology that can monitor network traffic in real-time, allowing the identification of suspicious behavior patterns that could indicate an attack. Thus, prevention and early detection measures are an integral part of the cyberattack mitigation strategy.

International cooperation plays an important role in addressing increasingly complex global cyber threats. Indonesia is involved in various multilateral initiatives such as the ASEAN Cybersecurity Cooperation Strategy and other international forums that discuss cybersecurity issues. Through this cooperation, member countries can share intelligence information on cyber threats, the latest attack techniques, and effective mitigation strategies .

The importance of international cooperation is also seen in efforts to build the capacity of developing countries in dealing with cyber threats. Indonesia participates in training programs and workshops organized by international organizations to improve technical and managerial capabilities in the field of cybersecurity. In addition, cooperation with the private sector is also key in building a stronger cybersecurity ecosystem. Dialogue between government and industry through Public-Private Dialogue (PPD) helps create more relevant policies and supports information exchange between the public and private sectors. International collaboration not only strengthens national defenses but also creates a global network to collectively counter cyber threats.

The Role of Migration Control in Maintaining National Resilience

Migration control, especially the management of the flow of passengers in and out at Immigration Checkpoints (TPI), is one of the important aspects of national resilience that goes far beyond just immigration administrative services. National resilience in this context has to do with the ability of states to maintain sovereignty, security, and social stability through effective surveillance of the movement of people across borders. Strong migration controls ensure that only individuals who meet legal requirements and do not pose a security threat can enter or exit the country's territory, thus preventing the entry of illegal immigrants,

smuggling, as well as the potential misuse of documents that could threaten domestic security.

In situations where migration control systems are weak or disrupted, such as when national data infrastructure is disrupted, migration flows become difficult to control. This has the potential to open a loophole for the entry of unproperly verified foreigners, which can carry the risk of cross-border crimes, including drug smuggling, human trafficking, and other illegal activities. The broader impact is the reduced ability of the state to maintain social and political stability, which ultimately undermines overall national resilience.

In addition, effective migration controls also play a role in supporting selective policies that allow the entry of foreigners that benefit and do not threaten the security of the country. This policy requires cross-agency synergy and strengthening of migration infrastructure so that supervision can be carried out comprehensively and accurately. Thus, migration control is not only a matter of administrative procedures, but part of a national strategy to maintain state sovereignty, prevent external threats, and ensure that domestic security and order are maintained.

The disruption to the National Data Center (PDN) due to the Brain Cipher ransomware attack has a direct impact on the services of the Immigration Checkpoint (TPI), especially at Soekarno-Hatta Airport. The immigration system, which is usually integrated and automated, has come to a complete halt since June 20, 2024, so the screening of passengers—both Indonesian citizens and foreigners—must be carried out manually. As a result, there are long queues and passenger build-up at the immigration checkpoint because the data verification process is very slow and inefficient.

During the disruption, thousands of international passengers were affected every day, with much longer than usual screening waiting times. To overcome the backlog, the Directorate General of Immigration added around 100 personnel at Soekarno-Hatta Airport, but this solution still cannot replace the speed and efficiency of the digital system. In addition to slowing the flow of passengers in and out, the issuance of important immigration documents such as passports and residence permits is also hampered, causing administrative delays for Indonesian citizens and foreigners that have an impact on mobility, tourism, and cross-border economic activities. This disruption highlights the immigration system's high reliance on reliable and secure digital infrastructure. As long as the PDN system has not yet recovered, immigration services will only be able to run normally after the emergency migration to Amazon Web Services on June 22–23, 2024. This incident is proof of the importance of strengthening reserves and emergency protocols so that vital services at TPI are not paralyzed due to similar cyber attacks in the future.

CONCLUSION

Cybersecurity is a crucial issue in the digital era, especially in national security. Threats such as malware, ransomware, and phishing lurk, with Indonesia recording 1.6 billion cyberattacks in 2021. Cyberattacks can cripple public services, steal sensitive data, and disrupt critical infrastructure. The National Data Center

(PDN), which functions as a center for storing and processing government data, is also an easy target. The ransomware attack that hit PDN in June 2024 paralyzed the immigration service at Soekarno-Hatta Airport. As a result, there are long queues at immigration checks because the checking system has to be done manually, so the process becomes much slower. In addition, flight schedules were also disrupted because passengers took longer to go through the immigration process. The lack of strict regulation exacerbates the situation, creating public distrust of the security of personal data. Collaboration between governments, the private sector, and communities is needed to address these challenges. The government has implemented the ITE Law, but education about cybersecurity is still lacking. Cooperation with international institutions can help Indonesia in implementing effective cybersecurity practices. With comprehensive regulations and good implementation, national security and public trust in digital systems can be improved.

REFERENCES

Adristi, Fikri Irfan, and Erika Ramadhani. "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya." Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen 2, no. 6 (2024): 196–212. https://journal.uii.ac.id/selma/article/view/35529.

Agung, Muhammad, Al Affan, Mona Fronita, Eki Saputra, Muhammad Luthfi Hamzah, Universitas Islam, Negeri Sultan, and Syarif Kasim. "MEASURING THE LEVEL OF CYBERSECURITY AWARENESS OF SOCIAL MEDIA USERS AMONG STUDENTS PENGGUNA MEDIA SOSIAL DI KALANGAN MAHASISWA." JURNAL INOVTEK POLBENG - SERI INFORMATIKA 10, no. 1 (2025): 134–45.

Al Ihsan, R., & Sekti, B. A. (2024). Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia. Prosiding SISFOTEK, 8(1), 7-11.

Bank Indonesia. "Manajemen Risiko Keamanan Siber Bank Umum Departemen," 2021, 75.

Budiyanto, D., & Mabruri, M. (2025, February). PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL:: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA. In Prosiding Seminar Nasional Sains dan Teknologi" SainTek" (Vol. 2, No. 1, pp. 981-994).

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., ... & Virgio, V. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135-1145.

Dewan Teknologi Informasi dan Komunikasi Nasional. "Pengembangan Keamanan Siber Nasional." Policy Paper, 2018, 1–30.

Framing, Analisis, Zhongdan Pan, and D A N Gerald. "KOSICKI DALAM PEMBERITAAN PERETASAN AKUN PUSAT DATA NASIONAL (PDN) DI MEDIA ONLINE TEMPO." Journal of Education Research 5, no. 3 (2024): 68–84.

Gabriel, Alza. "Perlindungan Hukum Atas Data Pribadi Dalam Kasus Kebocoran Data Pusat Data Nasional Sementara (Pdns) Dalam Perspektif Hukum Pidana." Seminar Nasional Hukum Dan Pancasila 3 (2024): 18–26.

Hanantyo, B., & Susanto, T. D. (2022). Kajian Potensi Penerapan Teknologi Smart Airport di Bandara Internasional Soekarno-Hatta Jakarta Indonesia. @ is The Best: Accounting Information Systems and Information Technology Business Enterprise, 7(1), 61-75.

Herlambang, Penggalih Mahardika, Sylvia Anjani, Hendro Wijayanto, and Murni Murni. "Cyber Security Behavior Model on Health Information System Users During Covid-19 Pandemic." Cyber Security Dan Forensik Digital 3, no. 2 (2020): 27–33. https://doi.org/10.14421/csecurity.2020.3.2.2152.

Julianto, Andhika Sigit, Ira Rosianal Hikmah, and Ray Novita Yasa. "Cyber-Risk Management Menggunakan NIST Cyber Security Framework (CSF) Dan Cobit 2019 Pada Instansi XYZ." Info Kripto 18, no. 2 (2024): 41–47. https://doi.org/10.56706/ik.v18i2.99.

Kairupan, Vetrisya Alvionita, and Atep Aulia Rahman. "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung." Jurnal Darma Agung 30, no. 1 (2022): 1164. https://doi.org/10.46930/ojsuda.v30i1.3167.

Kristianti, Novera, Ririn Kurniasi, Universitas Palangka Raya, and Riwayat Jurnal. "Peraturan Dan Regulasi Keamanan Siber Di Era Digital." Satya Dharma: Jurnal Ilmu Hukum 6055, no. 1 (2024): 297–310. https://ejournal.iahntp.ac.id/index.php/satya-dhamat.

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia. Jurnal Keamanan Nasional, 3.

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. EKSISBANK (Ekonomi Syariah dan Bisnis Perbankan), 8(1), 76-91.

Mustikasari, W., Dohamid, A. G., & Cempaka, F. G. (2025). Strategi Pertahanan Non Konvensional Indonesia dalam Menangkal Ancaman Siber Asimetris: Studi Kasus Serangan terhadap Infrastruktur Kritis. AURELIA: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia, 4(1), 1537-1544.

Mudra, Cakra, and Fragmadio Gana Prasidya. "Cybersecurity Dan Tata Kelola Intelijen." Jurnal Kajian Stratejik Ketahanan Nasional 7, no. 1 (2024). https://doi.org/10.7454/jkskn.v7i1.10086.

Mutiarachim, Atika, Aditya Putra Ramdani, Ahmad Zubair, Yohana Maritza, Program Studi, Bisnis Digital, Fakultas Ekonomika, Program Studi, Teknologi Informasi, and Fakultas Teknik. "Manajemen Risiko Digital Untuk Keamanan Siber Yang Lebih Kuat Di Era Industri 4 . 0- Systematic Literature Review (IoT), Kecerdasan Buatan (AI), Big Data , Dan Sistem Siber-Physical . Transformasi Ini Terlindungi , Yang Pada Akhirnya Mengancam Kelangs." Digital Business Intelligence Journal 1, no. 1 (2025): 54–66.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1), 8-16.

Nurul, Shinta, Shynta Anggrainy, and Siska Aprelyani. "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)." Jurnal Ekonomi Manajemen Sistem Informasi 3, no. 5 (2022): 564–73. https://doi.org/10.31933/jemsi.v3i5.992.

Prakesti, I. C. (2023). Nasionalisme dalam Ketahanan Nasional. Jurnal Pancasila dan Bela Negara, 3(1).

Ramadhani, E. H., Enriko, I. K. A., & Sari, E. L. I. P. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional. Jurnal Indonesia: Manajemen Informatika dan Komunikasi, 6(1), 570-580.

Ramadoni, Sofwan Rizko, Reza Pramasta Gegana, and Kalen Sanata. "Sejarah Undang-Undang ITE: Periodisasi Regulasi Peran Negara Dalam Ruang Digital." Langgong: Jurnal Ilmu Sosial Dan Humaniora 3, no. 2 (2023): 41–58.

Ramadhan, Y. A., & Reynaldy, R. (2024, July). Analisis Ancaman, Metode dan Mitigasi dalam Keamanan Privasi Data di Internet. In Prosiding Seminar Nasional Informatika (Vol. 2, pp. 607-614).

Runturambi, Arthur Josias Simon, and Samuel Hartawijaya Kusdiarto. "Analisis Ancaman Dan Adaptasi Unit Intelijen Djbc Dalam Mendukung Ketahanan Nasional Di Bidang Ekonomi Dalam Perspektif Intelijen Strategis (Threat Analysis and Adaptation of Djbc Intelligence Unit in Supporting National Resilience in the Economic Field W." Jurnal Lemhannas RI 11, no. 1 (2023): 58–71.

Samad, Y.S & Persadha, P.D. "Pendekatan Intelijen Strategis Sebagai Upaya Memberikan Perlindungan Di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat." Kajian 27, no. 1 (2022): 31–42.

Samad, M Yusuf, and Pratama Dahlian Persadha. "Memahami Perang Siber Rusia Dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats." Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi 24, no. 2 (2022): 135–46. http://dx.doi.org/10.17933/iptekkom.24.2.2022.135-146.

Sutisna, and Muhammad Syahroni Rofii. "Intelijen Strategis BAKAMLA RI Dalam Melaksanakan Kolaborasi Institusi Keamanan Maritim Untuk Ketahanan Nasional." Jurnal Kajian Stratejik Ketahanan Nasional 5, no. 1 (2022): 4–19. https://doi.org/10.7454/jkskn.v5i1.10058.

Susanto, M. (2021). Nasionalisme dan Ketahanan Nasional. Caritas pro Serviam, 43(01).

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada Data PDN Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. JOURNAL SAINS STUDENT RESEARCH, 2(6), 324-331.

Vimy, T, S Wiranto, R Rudiyanto, P Widodo, and ... "Ancaman Serangan Siber Pada Keamanan Nasional Indonesia." Jurnal … 6, no. 1 (2022): 2319–27. http://journal.upy.ac.id/index.php/pkn/article/view/2989.

Wibisono, G., Gultom, R. A., & Mantoro, T. (2024). Strategi Peningkatan Kapabilitas Satuan Siber Dispamsanau Melalui Pemanfaatan Artificial Intelligence Pada Keamanan Siber Berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1. Jurnal Review Pendidikan dan Pengajaran (JRPP), 7(1), 968-975.

Wulansari, Eka Martina. "Konsep Dan Urgensi Kemandirian Lembaga Keimigrasian Indonesia." Yustisia Tirtayasa : Jurnal Tugas Akhir 3, no. 3 (2023): 235. https://doi.org/10.51825/yta.v3i3.21927.