**Jurnal Ilmu Sosial dan Pendidikan (JISIP)**
Vol. 9 No. 3 Juli 2025
*e-ISSN : 2656-6753, p-ISSN: 2598-9944*
DOI: *10.36312/jisip.v9i3.8709/http://ejournal.mandalanursa.org/index.php/JISIP/index*

# Implementation of Cyber Policy in Indonesia: Study of Data Hacking Control by BSSN, Dittipidsiber, and the Ministry of Communication and Information at BPJS Health in 2021

**Rayhan Alevrido[1], Julian Aldrin Pasha[2]**
Universitas Indonesia

**Article Info**
***Article history:***
Received: 8 May 2025
Publish: 1 July 2025

***Keywords:***
*Implementation;*
*Cyber Policy;*
*Data Hacking.*

**Abstract**
*The BPJS Kesehatan data hack in 2021 shows important issues in the implementation of cybersecurity policies in Indonesia, especially regarding how effective coordination between institutions is. This study investigates how the response to the incident was affected by the lack of synchronization between the National Cyber and Crypto Agency (BSSN), the Directorate of Cyber Crime (Dittipidsiber) of the National Police Criminal Investigation Unit, and the Ministry of Communication and Informatics (Kominfo). This study uses a qualitative approach with a case study research type. The results of this study found that the process of mitigating data leaks became more difficult due to fragmentation of tasks, overlapping authorities, and the absence of an integrated crisis response protocol, although each institution has specific tasks, the lack of coordination led to slow and inefficient responses. In addition, systemic vulnerabilities increased because sectoral policies were not in line with national strategies.*

***Corresponding Author:***
**Rayhan Alevrido**
Universitas Indonesia
Email: rayhan@gmail.com

## 1. INTRODUCTION

The cybersecurity sector faces many challenges due to globalization and advances in digital technology (Toron, 2024). The increasing incidence of cybercrime in Indonesia, including hacking of public service data, demands strong policies. The BPJS Health data hacking case in 2021 shows that there are problems with the cyber security system and coordination between agencies responsible for data security.

In the ever-growing digital era, there are major threats to data security. Data is a valuable asset for organizations and individuals, and failure to protect it can result in financial, reputational and other harm. Data hacks, malware attacks, and identity theft are threats. Data hacking attacks can lead to unauthorized access to sensitive data such as customer personal information or financial information. A successful attack can cause data leaks, financial losses, and bad reputation for the organization (Sibarani, 2023).

In the era of increasingly digitalization, managing the personal data of JKN participants is very important for providing health services. By managing more than 98% of Indonesia's population, BPJS must prioritize data security and privacy. Data protection failures, such as those caused by cyber-attacks or negligence, can damage finances and public trust (Datik.com).

It cannot be denied that technological advances have made many things easier in modern times, such as managing JKN participant data. However, this convenience also means a big responsibility in protecting participants' personal information stored in health facilities and in the BPJS Health information system. With funding partly from the APBN, BPJS Health is responsible for maintaining participant data. As a personal data controller, BPJS Health is subject to the Personal Data Protection Law.

CNBC Indonesia reported several cyber-attacks on the public service sector in 2021. One of them was a cyber-attack that allegedly occurred on the Social Security Administering Agency (BPJS) website, bpjs-kesehatan.go.id, in May 2021. Around 279 million Indonesian population data was leaked as a result of the attack, and an account called "Kotz" on the online forum Raid Forums was sold for 0.15 bitcoin. In the end, Kominfo recommended that the link used to download personal data be stopped and the Raids Forum be blocked to prevent further spread of information.

Referring to the 2021 BPJS Health data leak case, it shows the importance of collaboration between the three main institutions, namely BSSN, Dittipidsiber, and the Ministry of Communication and Information. BSSN is technically responsible for cyber incident detection, protection, and recovery, but has no law enforcement or regulatory policy authority. Dittipidsiber handles investigations and law enforcement against cybercrime, they rely on technical data from BSSN and cannot make regulations. Meanwhile, Kominfo does not carry out operations or investigations, but functions as a regulator that sets digital security rules and standards.

The 2021 BPJS Health data hacking case revealed weak coordination between BSSN, Dittipidsiber and Kominfo. Although each of the three had different tasks, such as technical, law enforcement, and regulatory, the inability to work together led to a slow and ineffective response. There is no strong security audit mechanism, data exchange is inefficient, and cooperation is sectoral. As a result, there is insufficient control over BPJS Health's responsibility for leaks of its citizens' data. Additionally, there is no public transparency about the reasons for the hack and the steps taken to fix it.

BSSN, Dittipidsiber, and Kominfo have an important role in securing national digital infrastructure. The three central sectoral agencies each have duties and functions in accordance with the mandate of law or policy. Basically, policy implementation in each sectoral agency can involve the power, interests, strategies of the actors involved, institutional characteristics, authorities, compliance, and responsiveness to field conditions, so that each sectoral agency feels that it has different institutional powers and interests in certain situations.  It is at this level that birth occurs *incongruent* between BSSN, Dittipidsiber, and Kominfo in carrying out tasks in the field.

Based on these problems, this research aims to analyze how *incongruent* influencing the implementation of cyber policy in Indonesia, especially in handling the 2021 BPJS Health data hack.

## 2. RESEARCH METHOD

This research uses a qualitative approach, with the type of research method used in this writing being a case study. This research focuses on *incongruent* in implementing cyber policies between BSSN, Dittipidsiber and Kominfo agencies in handling data hacking that occurred at BPJS Health. Case studies allow researchers to collect data in various ways to obtain comprehensive information. Based on this, the data collected in this research was carried out using visual materials, documentation, interviews, structured and unstructured observations, and efforts to create protocols for recording and recording information (Creswell, 2016).

## 3. RESULTS AND DISSCUSION

### National and Sectoral Cyber Policy

Over the past twenty years, Indonesia has experienced rapid digital transformation, which has resulted in a dynamic technology ecosystem but one that is also vulnerable to cyber threats. More and more people are relying on electronic systems, in both the public and private sectors, making data leaks, hacking and disinformation a very important problem for governments. In situations like this, sectoral and national cyber policies are very important for the security of Indonesia's digital space.

Since Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which was later revised into Law Number 19 of 2016, Indonesia's cyber policy has experienced significant developments. This was an early law used to manage electronic systems and protect user data. However, various sectoral technical regulations such as PP Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions and Minister of Communication and Information Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems were created in response to the limitations of the ITE Law in dealing with complex cyber security issues.

In 2017, Presidential Regulation Number 53 of 2017 which established the National Cyber and Crypto Agency (BSSN), which was then strengthened by Presidential Decree Number 28 of 2021, brought major changes to national cyber policy. To develop a national cyber security strategy, establish national information security standards, and manage *National Cyber Security Operations Center* (NCSOC) to detect, respond and mitigate cyber incidents, BSSN functions as the main coordinator of the national cyber security system. Choucri and Goldsmith (2012) emphasize that cyber policies must be able to address the anonymous, cross-border and open features of digital spaces. Therefore, cyber security policies must be proactive, integrated and cross-agency rather than sectoral and reactive.

Indonesia's sectoral cyber policy is still very fragmented. Each sector partially adopts rules, guidelines and security protocols in accordance with institutional authorities. This was proven in the case of BPJS Health data hacking in 2021, which is the focus of the research in this article. BSSN, Dittipidsiber Bareskrim Polri, and the Ministry of Communication and Information are the three main institutions responsible for handling these cases, but implementation in the field often overlaps.

BSSN functions as the technical authority and coordinator of the national security system, especially in terms of improving the country's vital information infrastructure (IIVN) and developing security technical standards. At Dittipidsiber Bareskrim Polri, law enforcement, digital forensic investigations, and collection of electronic evidence related to cybercrimes are carried out. As a regulator of the information and communications sector, Kominfo is responsible for establishing technical regulations, supervising PSE (Electronic System Operators), and increasing public digital literacy. According to Bayuk et al. (2012), good cyber policy includes not only regulations, but also practices, institutional roles, and communication systems between actors that can be implemented in *cyber governance*. In the case of BPJS Health, overlapping digital forensic authorities, unsynchronized public communications between agencies, and unclear incident investigation protocols indicate a lack of coordination.

Kristianti and Kurniasi (2024) show that cyber security management performance is greatly influenced by effective incident response, system interoperability, and transparency of the chain of command in digital emergency situations. These three components still represent structural challenges in Indonesia's current policy architecture. It is very important as a response to form *National Cyber Incident Response Protocol* (NCIRP) to regulate cyber incident management in an integrated manner. NCIRP will define agency roles and responsibilities in the technical, legal, regulatory, and public communications areas. The appointment of BSSN as the main national coordinator with legally strengthened authority can avoid command dualism and improve responses to cyber-attacks.

Several countries, such as Singapore, Estonia and South Korea, have used the approach of whole-of-government and whole-of-society for their cyber policies. This method involves the government, private sector, academics and civil society in forming a national digital security plan. By increasing cross-sector participation in policy formulation and implementation of national security audits, Indonesia can learn lessons from these international practices. As in the research of Meher et al. (2023), public sector cyber resilience is supported by general awareness and data security practices implemented at all levels of the organization, as well as technical capabilities.

**Data Hacking at BPJS Health**

One of the biggest cyber events in Indonesia was the data hack that hit the Health Social Security Administration (BPJS) in 2021. This attracted widespread public attention and forced state institutions to act, especially in terms of cyber security. This situation shows that there are significant vulnerabilities in government data security systems, which protect the data of millions of people. In the online forum RaidForums in May 2021, it was reported that data on more than 279 million Indonesians, including NIK, addresses, telephone numbers and health data, had been leaked and traded illegally. The perpetrator stated that he had access to the BPJS Health database and sold the data to interested parties. Several sources later verified this information, including independent cyber security communities such as Indonesia Leaks and Cyberthreat.id, which showed that many of the leaked data samples were very similar to real data from the Indonesian people.

This situation shows structural weaknesses in the cybersecurity management of government organizations. Because BPJS Health stores personal data, they must have strict data protection protocols and comply with modern standards of cyber *hygiene*. In this context, Andress and Winterfeld (2014) stated that important state information systems must be built using a defense-*in-depth*, namely layers of defense that focus on early detection, rapid response, and effective incident recovery. The national cyber security policy implemented by the National Cyber and Crypto Agency (BSSN), the Directorate of Cyber Crime, Bareskrim Polri (Dittipidsiber), and the Ministry of Communication and Information (Kominfo) was also tested by this data hack. Based on a study conducted by Disantara (2021), factors that increase the possibility of public data leaks include a lack of collaboration between institutions, a lack of technical standards for information security in government institutions, and poor supervision of third parties (IT vendors).

In addition, from a legal perspective, this data leak occurred when the Personal Data Protection Law (UU PDP) had not yet been passed in parliament at that time. This condition creates legal loopholes that hamper law enforcement efforts against cybercriminals and negligent data management institutions. In Solove's (2008) view, countries must implement strong regulations to protect human rights to protect personal data, because it is not just a technical issue.

Public trust in government data management institutions declined as a result of this hack. Many people question the government's commitment to keeping its citizens' personal data safe and confidential. Additionally, this event shows how important it is to improve *cyber resilience* nationally, namely the country's ability to prevent and recover from cyber-attacks quickly. The BPJS Health data hacking incident provides an important lesson that national digital transformation must be accompanied by strengthening cyber security infrastructure, increasing human resource capacity, and harmonizing policies between institutions. Indonesia cannot handle increasingly complex and multidimensional cyber challenges unless it adopts a holistic and collaborative approach.

**Inter-Agency Coordination in Handling Data Hacking**

Coordination between institutions is a crucial element in national cyber governance, especially in responding to large-scale data hacking incidents such as what happened to BPJS Health in 2021. In this context, the collaborative role between the National Cyber and Crypto Agency (BSSN), the Directorate of Cyber Crime (Dittipidsiber) Bareskrim Polri, and the Ministry of Communication and Informatics (Kominfo) is key in determining the effectiveness of handling incidents and restoring public trust.

Presidential Regulation no. 28 of 2021 concerning BSSN mandates BSSN as the main institution responsible for regulating cyber security in Indonesia, based on the national policy structure. However, in practice, institutional coordination still faces a number of problems. These include misaligned authorities, delays in information dissemination, and the absence of a comprehensive system to control cyber emergencies. The study by Nirwana et al. (2024) emphasizes that in the case of cyber crises, such as personal data leaks, reactions between institutions usually proceed in institutional silos, which causes the mitigation process to be slower and less synergistic.

The three state institutions each responded to the BPJS Health case. BSSN conducted a security system audit and provided technical advice, Dittipidsiber conducted a digital forensic investigation into the source and perpetrator of the leak, and Kominfo issued a public statement and encouraged blocking and communication actions. However, the three do not necessarily form a unified crisis command center (*cyber incident response center*) which is organized *real-time*. This is different from the habits in other countries that have *Computer Security Incident Response Team* National (CSIRT) which is centralized and works cross-sectorally and multi-level with a centralized structure.

Carr's (2016) study of national cyber security shows that in the era of network-based cyber security threats, a fragmented response will only worsen the impact of incidents and open up opportunities for further attacks. Therefore, cyber security must be carried out carefully of whole-of-government and whole-of-society by involving state agencies, the private sector, and digital security groups working together. Formation of Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) in Indonesia was previously intended to assist technical coordination between sectors, but after being merged into BSSN, there were still coordination problems, especially related to unclear communication channels and reporting systems. A study by Chang and Coppel (2020) underscores that building a strong cybersecurity coordination system requires institutional capacity, system interoperability, and standardized crisis response protocols.

In addition, sectoral cybersecurity policies do not fully follow national policies. Ministries and sector agencies such as BPJS Health continue to develop their own IT security protocols without reference to the National Cybersecurity Strategy from BSSN. This increases the risk of systemic vulnerabilities and reduces the sector's readiness for cyber threats.

To improve inter-agency coordination in cyber security, it is necessary to focus on establishing a National Cyber Crisis Management Center which must be cross-sectoral and rely on system event control protocols. This model has been used effectively in several countries, such as Singapore through the CSA (Cyber Security Agency) and Estonia through CERT-EE, which combines civil, intelligence and technical authorities in one integrated framework. Normatively, this coordination problem shows that cyber security is a matter of governance, institutional coordination, and crisis leadership in addition to technology. In this situation, it is important to emphasize the importance of an institutional framework that can assist the exchange of information, harmonization of procedures, and a culture of cooperation between institutions that previously worked within their respective sectoral logics.

## 4. CONCLUSION

The BPJS Health data hacking case in 2021 shows that there are big problems in implementing cyber security policies in Indonesia, especially regarding how effective cooperation between institutions is. In national cyber policy, the National Cyber and Crypto Agency (BSSN), the Directorate of Cyber Crime, Bareskrim Polri (Dittipidsiber), and the Ministry of Communication and Information (Kominfo) each have special tasks. However, experience in the field shows that a lack of cooperation between agencies can worsen the handling of large-scale cyber incidents. The process of mitigating data leaks is hampered by a number of problems, including overlapping authority, misalignment of tasks, and communication and response systems that are not integrated.

This research shows that institutional reform must be prioritized in efforts to increase national cyber resilience, one way to do this is by establishing the National *Cyber Crisis Management Center*. This center must be able to integrate technical, legal, regulatory and public communication tasks in one integrated command system. In addition, strategic steps taken to increase responsiveness to future digital threats include strengthening the BSSN coordination authority and implementing a whole-of-government and whole-of-society in cyber policy. The BPJS Health care provides an important lesson that national digital transformation must be accompanied by cyber governance reform based on institutional interoperability, human resource capacity, and cross-sector regulatory harmonization.

## 5. REFERENCE

Andress, Jason, and Winterfield Steve. 2014. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham:Syngress.

Badan Siber dan Sandi Negara, Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019.

Carr, Madeline. 2016. US Power and the Internet in International Relations: The Irony of the Information Age. London: Palgrave Macmillan.

CATRA. "Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional". Majalah Setjen Wantannas, Edisi VI September 2016.

Chang, Lennon Y.C., and Coppel, Nicholas. 2020. Building cyber security awareness in a developing country: Lessons from Myanmar. Vol. 97.

Choucri, Nazli, and Goldsmith, Daniel. 2012. Lost in cyberspace: Harnessing the Internet, International Relations, and Global Security. Vol. 68., No. 2.

Creswell, John W. 2016. Pendekatan Metode, Kualitatif, Kuantitatif, dan Campuran, Edisi Keempat. Yogyakarta: Pustaka Pelajar.

Cyberthreat.id. (2021). "279 Juta Data WNI Bocor, Diduga dari BPJS Kesehatan.". https://cyberthreat.id/

Disantara, Fradhana Putra. 2021. Tripartite Collaborative Institutions: Skema Konvergensi Institusi Untuk Mewujudkan Ketahanan Siber Indonesia. Vol. 18., No. 2.

IndonesiaLeaks. 2021. "Investigasi Kebocoran Data BPJS". https://indonesialeaks.id/

Kristianti, Novera, dan Kurniasi, Ririn. 2024. Peraturan dan Regulasi Keamanan Siber di Era Digital. Vol. 7., No. 1.

Nirwana, Dwi, Ely Nurjannah, Charoline Renta Anggirani Marpaung, dan Hansein Arif Wijaya. 2024. Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. Vol. 7., No. 7.

Sibarani, Blasius Erik. 2023. Ekonomi dan Bisnis Digital. Sukoharjo: Pradina Pustaka.

Solove, Daniel J. 2008. Understanding Privacy. Harvard University Press.

Toron, Vinsensius Bawa. 2024. Sosiologi Pendidikan. Gowa: CV Ruang Tentor.