JHSS (Journal of Humanities and Social Studies)
https://journal.unpak.ac.id/index.php/jhss

Volume 09, Number 01, Page 028-038
e-ISSN: 2598-120X; p-ISSN: 2598-117X

POLITICAL WILL OF THE INDONESIAN GOVERNMENT IN ADDRESSING DATA LEAKAGE AND CYBERSECURITY IN THE ERA OF DIGITAL TRANSFORMATION

Safrida Nurulita [a*], Ridwan [a)]

[a)] *Universitas Pembangunan Nasional "Veteran" Jakarta, Jakarta, Indonesia*

[a*)] *safridanurulita@gmail.com*

Article history: *received 27 May 2025; revised 10 June 2025; accepted 18 June 2025* *DOI: https://doi.org/10.33751/jhss.v9i1.33*

Abstract. Technological development requires everyone to carry out activities in cyberspace. Cybercriminals exploit the exchange of information to steal important data, which indirectly contributes to data leakage. Indonesia is one of the countries with the most internet users in the world and often experiences data leaks. Therefore, the risk of cyber threats coincides with technological use. This research discusses the extent of the Indonesian government's political will to overcome cyber threats. The research method used is a descriptive qualitative type that uses Brinkerhoff's political will theory. The results show that the Indonesian government is strongly committed to overcoming cybersecurity threats and data leaks through the establishment of the BSSN and regulations, coordination with various parties, policy monitoring, and human resource development. However, weak security awareness among policymakers and the public, gaps in cybersecurity education and understanding, budget limitations, weak cybersecurity systems, and sectoral egos present challenges to strengthening cybersecurity in Indonesia and cause data leaks. Thus, the government's concrete steps to establish the Cyber Security and Resilience Bill are expected to fill the regulatory vacuum so that the implementation of cyber security policies can be optimized. Increasing government security awareness, prioritizing the cybersecurity budget, ensuring the availability of competent resources, conducting well-coordinated efforts, providing education, and encouraging active community involvement are solutions that can protect data from growing threats.

Keywords: political will; cybersecurity; data leakage

I. INTRODUCTION

The development of the current era can be called the era of digital transformation because the use of Information and Communication Technology (ICT) has changed various fields of human activity. This change can be characterized by the emergence of information technology that is growing rapidly and sophisticated, such as artificial intelligence to the Internet of Things (IoT). Digital transformation has made it easier for everyone to obtain information from anywhere and anytime, positively crushing crucial sectors such as the economy, education, government, defense, and security. On the other side, the development of digital transformation can be used by unauthorized parties to hack, steal, damage, and even sell data stored in cyberspace.

The survey results by the Indonesian Internet Service Providers Association (APJII) present the number of internet users in Indonesia reaching 221,563,479 people or 79.5% of the total population of Indonesia, which reached 278,696,200 people in 2024. The number increased by 1.4% compared to the previous year, which is in 2023 the internet penetration rate in Indonesia was 78.19%. Survey results by Surfshark, a virtual private network (VPN) company from the Netherlands, stated that Indonesia is the 8th country in the world with the most data leaks, reaching 94.22 million leaked accounts from January 2020 to January 2024. Data leaks are increasing because only about 64% of government institutions have information security technology [1].

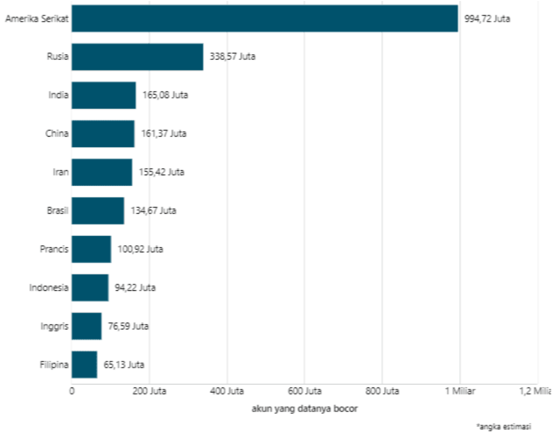

Figure 1. The biggest data leaks in 10 countries (January 2020-January 2024)

Based on the Indonesian Cyber Security Landscape 2023 data below, the National Cyber and Crypto Agency (BSSN) shows that throughout 2023 there were 403,990,813 cyber anomalies that entered Indonesia, where the highest anomaly was in August, namely 78,464,385 and the lowest anomaly was in November, namely 19,296,439. Based on the

Cybersecurity Monitoring Monthly Report 2024 shows that from January to September, the largest number of anomalies occurred in September, which amounted to 21,927,579 that can potentially become cyberattacks. Seeing the high number of incoming traffic anomalies followed by the increasing internet penetration in Indonesia, the government should pay attention to cybersecurity to protect national and personal data, because data leaks can threaten the stability of the country in various aspects.

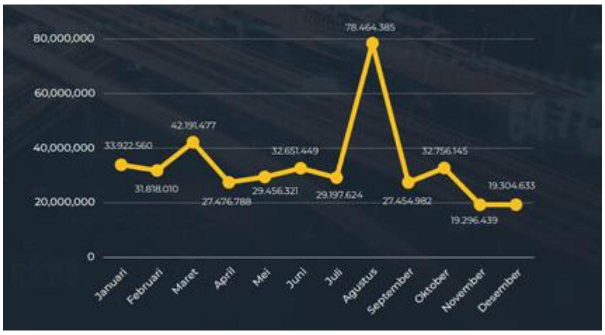

Figure 2. Total anomalous traffic in Indonesia during 2023

Massive developments in the digital transformation era followed by the increase in internet users can cause potential threats to cybersecurity [2]. The International Telecommunication Union (ITU) in the ITU-T X.1205 document recommendation defines cybersecurity as a set of tools, policies, security concepts, security protection, guidelines, risk management approaches, actions, training, best practices, assurances, and technologies used to protect the cyber environment, organizations, assets, and users, including connected computer equipment, personnel, infrastructure, applications, services, telecommunications systems and all information transmitted and/or information stored within the scope of cyberspace. Cybersecurity always tries to ensure the safety of users from the risk of threats that can occur in the cyber environment.

In terms of cybersecurity, data security is a very important aspect, in accordance with the objectives of cybersecurity in general, namely: (1) availability, (2) integrity, which can include authenticity and irrefutability, (3) confidentiality [3]. Thus, cybersecurity can be classified as a High Politics issue [4]. This means cyber threats as a High Politics issue are seen by international countries as having a vital influence on state security and defense [5]. Especially if looking at cyber threats or traffic anomalies that enter Indonesia not only come from outside the country, but also within the country [6]. Based on data from the National Cyber Security Index (NCSI) in 2023, Indonesia ranks 49th out of 176 countries with a score of 63.64% and 5th in ASEAN in terms of cyber security [7], [8].

Cyber security in the digital transformation era is one of the challenges for state institutions because cyberattacks are able to paralyze public service systems that will have a direct impact on economic disruption. It is stated in the Regulation of the Minister of Defense Number 82 of 2014 concerning Cyber Defense that the impact of cyberattacks can cause (1) Functional disruption, (2) Remote control, (3) Misuse of information, (4) Riots, fear, violence, chaos, and conflict, and (5) Other conditions that are very detrimental, so it is possible to result in destruction. In line with this, the case of cyberattacks on the state recently repeated itself, which was on June 20, 2024 there was a disruption to immigration caused by ransomware attacking the Temporary National Data Center (PDNS) in Surabaya. As a result, several public service servers were paralyzed as a result of the attack [9].

TABLE 1. Data Leak Cases in Indonesia

No	Year	Data Leak Cases	Total Data
1	May 2020	User and merchant data of e-Commerce company Tokopedia was sold on the dark web. The leaked information included names, e-mail addresses, phone numbers, and passwords	91 million user accounts and over 7 million merchant accounts [10]
2	May 2021	BPJS Health user data. The leaked information includes NIK, name, address, phone number, and health data	More than 279 million [11]
3	September 2022	KPU DPT data sold by Hacker Bjorka on Breached Forums includes NIK, family card, name, place of birth, gender, and age	More than 105 million [12]
4	March 2023	BPJS Employment user data was again leaked by Hacker Bjorka and sold on the dark web	19,5 million [10]
5	November 2023	The 2024 general election permanent voter data was hacked from the KPU's Voter Data Information System (SIDALIH) by hacker Jimbo. The leaked data includes NIK, KK number, KTP number, name, gender, and so on	204 million [13]
6	September 2024	Taxpayer Identification Number (NPWP) data whose victims include important people such as the President of Indonesia, Jokowi and his two children, Minister of Finance, Sri Mulyani, Minister of Communication and digital, Budi Arie, and other important ministers whose data has been sold on the dark web	6,6 million [14]

The data leakage cases in the table above are examples of the many cyberattacks that have occurred in Indonesia, including attacks carried out by Hacker Bjorka which have shocked Indonesia several times. The handling and resolution of data leakage cases that are not transparent and continuously repeated have an impact on the decline in public trust in the government. The government's failure to protect data violates the fulfillment of rights in ensuring the protection of citizens' personal data from various threats that can harm their privacy.

The Indonesian government has enacted several regulations related to cybersecurity, including Law Number 19 of 2016 concerning amendments to Telecommunications Law Number 11 of 2008 concerning Electronic Information and Transactions as one of the efforts to deal with cybersecurity threats and which is a milestone in the formulation of other regulations and policies related to cyber defense, preventing articles that have multiple interpretations, and guaranteeing and respecting individual rights and freedoms. Furthermore, through Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency to replace Presidential Regulation Number 53 of 2017 concerning the National Cyber and Crypto Agency (BSSN), so that the implementation of organizational duties and functions can run optimally and more effectively and efficiently in the field of cyber and password security. Then, Law Number 27 of 2022 on Personal Data Protection which aims to ensure the protection of personal data as a citizen's right. Presidential Regulation Number 82 of 2022 on the Protection of Vital Information Infrastructure (VII) which aims to protect vital information infrastructure from disruption, damage, and threats of cyberattacks that have an impact on strategic sectors and strengthen cybersecurity through BSSN as the main actor in charge.

However, data leaks are still very often happening, which is very concerning, because the threat to state information data and personal data cannot be merely underestimated because it can be used for cybercrime. Unauthorized use of personal data can be done through various means such as fraud, extortion and leaking personal data, as well as using other people's data [15]. Unauthorized use of personal data caused by data leakage has proven to be detrimental to individuals such as being used for illegal online loans, being contacted by unknown parties, social media hijacking, and reduction of account and e-wallet balances [16], [17].

Cyber-attacks, such as phishing on the healthcare sector, in this case hospitals, have a crucial impact on disrupting operations, hampering patient services, financial losses due to paying ransoms to the attackers, as well as recovering, and so on. In addition, when the patient's personal data or medical history that is private is leaked, it will provide discomfort to patients who are treated and reduce their trust in the hospital [18], [19].

Similarly, cyberattacks that attack critical infrastructure and result in data leaks. The impact of cyber-attacks on the economic sector has caused losses not only to pay for the cost of restoring affected systems and infrastructure, but also to pay ransoms. Cyberattacks also cause operational disruptions that indirectly have a significant impact on productivity and loss of revenue. In 2023 Indonesia suffered a loss of 10 trillion just from ransomware attacks [20].

The cases of cyber-attacks that occurred in 1999 and 2013 to former Indonesian Presidents, B.J. Habibie and Susilo Bambang Yudhoyono had galvanized the nation, where transcripts of conversations between B.J. Habibie and Attorney General Andi Muhammad Ghalib were leaked to the public due to wiretapping. Later, the Australian Embassy also managed to wiretap several important officials in Indonesia, including SBY and his wife. The case is proof that there are vulnerabilities in Indonesia's cyber security defense that can disrupt political stability [21], [22]. Public officials and institutions in a country should use specialized communication tools that can guarantee the confidentiality of conversations in order to avoid wiretapping and cyberattacks.

Overcoming this situation is not easy because building political will related to cybersecurity threats is still faced with complex challenges. It is caused by the security system, commitment, and security awareness or awareness of the importance of cybersecurity to protect data from policy makers is still weak, which leads to data leaks [23]. Cybersecurity threats can be understood not only as a technical problem, but also as a strategic problem that requires involvement and cooperation between sectors such as the military, cyber defense and security agencies, in this case BSSN, other government agencies, the private sector, and the community. However, coordination among institutions still not optimal.

This situation causes national defense in the field of cybersecurity to not work properly, which makes Indonesia very vulnerable to attacks. In addition, the formation of policies regarding cybersecurity in Indonesia has not been clearly coordinated due to the lack of coherent regulations. Thus, the massive development of technology in Indonesia, supported by the rapid increase in internet users in the era of digital transformation, has not seen a balanced policy on cybersecurity.

A government's change in perspective on cybersecurity is needed as a form of political will, especially in the era of digital transformation, which requires the government to create concrete policies and allocate adequate resources. The success of cybersecurity-related policies depends not only on infrastructure and technical capabilities, but also on the political will of the government and other stakeholders in dealing with cybersecurity threats. Political will itself can be defined as the extent of commitment support among decision makers for certain policy solutions related to certain problems (Post et al., 2010) in Sarajevo [24]. In other words, political will is a commitment from the government, both executive and legislative, to take an action to deal with cybersecurity threats in the era of digital transformation.

Based on the description above, the author will discuss how the political will of the Indonesian government in overcoming data leakage and cybersecurity in the era of digital transformation. In conducting the research, the author also looks at how the National Cyber and Crypto Agency (BSSN) and the Ministry of Communications and Digital cope with cybersecurity challenges. Then, it will examine the extent to which political will is reflected in regulations and strategic actions taken to address evolving cyber threats.

II. RESEARCH METHODS

This research uses Creswell's qualitative research methods to provide an in-depth explanation of certain issues [25]. In this case, the author explains the phenomenon of data leaks and weak cybersecurity in Indonesia. This kind of descriptive qualitative research seeks to provide in-depth explanations and descriptions in words or narratives regarding the extent of the Indonesian government's political will in dealing with data leaks and cybersecurity in the era of ever-evolving digital transformation.

Qualitative data collection techniques carried out by the author are in-depth interviews using unstructured or open-ended interview methods to find out the answers to the problems asked, document review, and documentation in conducting research. This research uses primary and secondary data sources collected directly by the author. Primary data was obtained through interviews conducted with research subjects as key informants. Then, secondary data comes from the internet, documents, articles, books, and journals related to the research to support research data.

Last, the author used data analysis techniques according to Miles and Huberman (1984) in Creswell's book [25]. Miles and Huberman categorized the stages of data analysis, namely data reduction by determining which data to use, data display, which involves presenting the data found in the field, and conclusion drawing/verification, by considering the findings from the field and analyzing them with reference to documents, books, journals, or interview results to draw conclusions.

Brinkerhoff's theory of political will [26] which includes government initiative, policy selection, stakeholder mobilization, public commitment and resource allocation, credible sanctions, sustainability of efforts, and learning and adaptation, is the theory used by the author to answer the research questions. According to Brinkerhoff in Sarajevo (2015) [24] the basis of political will is formed from the bottom up as the key to the success of a policy. The author uses the theory of political will to further analyze the political will of the Indonesian government in overcoming cyber security threats, including increasing security awareness or awareness of the importance of security and data protection, so as to create a secure cyber space and minimize the leakage of personal, private, or national data. This theory will also examine whether the policies implemented by BSSN are running optimally.

III. RESULTS AND DISCUSSION

A. Cyber Security Threat Conditions

Cyber threats are a consequence of digitalization that is not accompanied by increased awareness and adequate cyber security systems. Every individual and organization faced with constantly changing cyber threats due to rapid technological advances [27]. Cyberattacks carried out irresponsibly can originate from state actors or non-state actors, including individuals, groups of individuals, organizations, and countries [28].

Cyber security threats pose a new challenge for countries, especially developing countries. Country must have cyber security preparedness in facing the era of digital transformation. The industrial revolution 4.0 has opened up a wide space for interaction in the virtual world, thereby creating negative impacts on national security. This has prompted countries to adapt by changing their legal, political, and strategic frameworks, including cybersecurity concepts and laws, as well as global cooperation toward shared security. Often, disparities in national security issues arise because developing countries are unable to address current issues, including the lack of adequate cybersecurity infrastructure and defense [22].

The High-Tech Crime Trends Report 2025 published by Group-IB states that Indonesia ranks second as the country with the highest number of Advanced Persistent Threat (APT) cyberattacks in the Asia-Pacific region in 2024. Indonesia accounts for 7% of the total 20% of incidents in the region. APT refers to attacks carried out by cyberattack groups or threat actors, whether state-affiliated or non-state actors [29].

The report reveals that ransomware is the most profitable form of cybercrime. These attacks increased by 10% globally in 2024, driven by Ransomware as a Service (Raas). There were 467 ransomware attacks in the Asia-Pacific region. Several sectors, such as the property industry, manufacturing, and financial services, were the main targets. The impact of ransomware attacks often includes extortion and large-scale data breaches, such as 5,066 ransomware cases that resulted in data breaches on Dedicated Leak Sites (DLS), with sensitive information belonging to companies and critical institutions leaked [29].

Indonesia and Thailand are among the top 10 countries with the largest global markets affected by data leaks on the dark web. Phishing attacks increased by 22% worldwide in 2024. This was caused by irresponsible parties stealing data. Deepfake technology generated by artificial intelligence (AI) has made it easier for cybercriminals to carry out phishing or fraud that looks more real and is difficult to detect [32]. BSSN also reported 2,487,041 APT activities, 514,508 ransomware activities, and 26,771,610 phishing activities that occurred in Indonesia in 2024 [6].

Cyber threats have caused geopolitical instability triggered by espionage and data leaks. Meanwhile, ransomware attacks also take advantage of data leaks, which together form an ever-evolving cyber threat dynamic. Country's ability to master technology is one of the key factors in overcoming cyber threats. This is because cybercriminals' methods and cyber threats evolve alongside rapid technological advances [22], [23], [30].

Not only that, cybercriminals often target the weakest points to enter the technological systems and infrastructure of organizations, companies, and governments to carry out attacks. They exploit gaps in outdated systems, weak security settings, and dependence on technology. These attacks aim to gain financial benefits and steal important information, which can damage reputation and lead to loss of consumer trust [31]. According to an interview with BSSN, cyberattacks pose a fatal threat to data. Unsecured networks can serve as a conduit for attacks, as all networks are interconnected. These attacks can also spread to other vital information infrastructures.

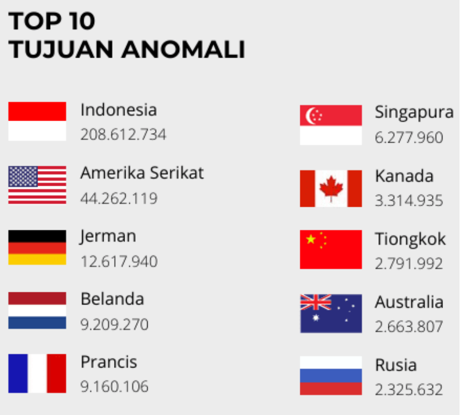

Figure 3. Top 10 destination countries of anomaly

The image above shows that Indonesia is the top destination for anomalies or countries targeted by suspicious activities that have the potential to be cyberattacks, with a total of 208,612,734 anomalies in 2023. In 2024, Indonesia will again be the top destination for anomalies, with a total of 194,562,390 anomalies. It is known that cybercrime is a form of crime that can transcend national borders [28].

Based on the 2023 Cyber Security Landscape report, referring to the results of monitoring and analysis conducted by Cyber Threat Intelligence, BSSN also conducted observations and found a total of 347 suspected cyber incidents. Data breach is the highest type of suspected cyber incident. Monitoring of the darknet found 1,674,185 data exposures that impacted 429 stakeholders in Indonesia. BSSN reported that 189 cases of web defacement were found on hidden pages. Based on this report, the three types of cyber incidents that were predominantly handled by BSSN during the implementation of cyber response assistance were web defacement, ransomware, and data breach [32].

In 2024, BSSN conducted another review and found 241 indications of data breach incidents from the results of observation and analysis of Cyber Threat Intelligence. The results of monitoring the darknet showed that 461 stakeholders in Indonesia were affected by data exposure, with a total of 56,128,160 findings. In the case of web defacement, 5,780 incidents were identified that had attacked various domains, with 4,071 of them related to online gambling and targeting government agency websites. The 2024 Cybersecurity Landscape Report states that there are five dominant types of cases handled by BSSN in cyber incident response assistance, namely Data Breach, Illegal Access, Web defacement, Ransomware, and Distributed Denial of Service (DDoS) [6].

Massive of cyber threats in Indonesia shows that the government's technological capabilities and skills in the cyber field still need to be improved, if compared to the capabilities of cyber criminals [30]. The state has a role in addressing these issues by having policies related to cyber security as a form of preparedness in facing threats. In line with an interview by SAFEnet, the government plays a significant role as it is responsible for protecting all Indonesian citizens, including in the context of cybersecurity. One step that can be taken is to develop a cybersecurity strategy through regulations and legislation. The involvement of various stakeholders in ensuring security in cyberspace is a form of awareness to protect citizens. Effective governance by the National Cyber and Crypto Agency (BSSN) in responding to cyber threats is crucial to maintaining national cyber security and resilience [33].

However, high cases of cyberattacks and data leaks show that regulations, implementation, roles, functions, and awareness from various parties are not yet optimal in dealing with national cyber threats. Cyber security enforcement tends to be sectoral, which is not well managed and synergized [28]. According to interviews with BSSN, awareness of the importance of information security is hindered by sectoral ego, such as some institutions' reluctance to coordinate, resource issues, and limited understanding in the regions, which often results in security steps not being followed properly.

Based on the 2024 Cybersecurity Landscape, BSSN predicts two potential cyber threats in 2025: social and technical threats. Social cyber threats include the spread of pornographic content, online gambling, online fraud, terrorism, disinformation, and misinformation, exacerbated by the potential misuse of AI technology. Additionally, technical cyber threats include web defacement, AI, phishing, malware, Advanced Persistent Threat (APT), Distributed Denial of Service (DDoS), and credential data theft.

Talking about cyber threats also means mentioning data leaks. In this era of digital transformation, privacy is very important because personal data is an individual's identity and markers. As time goes by, people are faced with the need to expose themselves to other individuals and organizations, which can be a challenge for protecting privacy [34]. Every activity in today's era is often done online, including financial transactions, work, and even communication that requires personal information. This ease of access can have a negative impact, one of which is the leakage of social media user data [17]. This also increases the risk of other cybercrimes such as identity theft, fraud, and account hacking.

Cases of personal data leaks, such as the leaks of KTP, NPWP, KPU data, and BPJS data, which have harmed many parties, have affected many Indonesians. Data breaches affecting individuals are often exploited by irresponsible parties. Based on interviews with participants, this is compounded by those who have experienced data breaches by receiving spam calls or phone calls from unknown individuals for promotional purposes, fraudulent activities, and the theft of personal data, including hacking, have suffered harmful psychological effects. Meanwhile, victims who have been hacked must create new accounts to feel safer.

Such forms of cybercrime directly infringe upon individual privacy.

Individual awareness of data security plays a major role in the community's ability to protect national sovereignty [35]. Interviews with SAFEnet revealed that it is important not only to ensure active community involvement in securing data, but also to encourage the community to pressure the government to ensure that cybersecurity procedures are implemented more effectively. Additionally, several preventive measures were taken to protect data include using strong passwords, enabling two-factor authentication (2FA), avoiding the use of public Wi-Fi networks without additional protection such as a VPN to prevent data theft, and checking app permissions before installing them to prevent unnecessary access to personal data. These measures are taken to feel safe when conducting activities in the digital space and to minimize the risk of data leaks.

Despite taking these preventive measures, the suboptimal data security system, coupled with weak regulations and unclear sanctions regarding data protection, has made data breaches prone to occur. Frequent data breaches indicate a disparity between data protection policies and cybersecurity measures and their implementation [11].

As data security is very important because it relates to privacy rights and personal data protection. Based on interviews with participants, this responsibility does not only lie with the citizens; the private sector also has a role as a service provider or infrastructure owner that is obliged to protect consumer and company data. On the other hand, political will is needed from the government to ensure public data security and its management in accordance with legal provisions.

Indonesia, which faces high cyber threats every year, needs to improve personal data protection for its citizens. The government must demonstrate a serious commitment to adapting to increasingly sophisticated technology and complying with international standards in protecting personal data [23]. Strict cybersecurity standards from the government, strong regulations, and heavy penalties for data breaches are necessary, accompanied by infrastructure improvements as a preventive measure to ensure that systems are not easily hacked. Additionally, the private sector must be transparent about their data privacy policies, promptly notify users of data breaches, and clearly communicate the impact and steps taken to address the issue. The government and private sector are expected to ensure the security of citizens' activities in the digital space by enhancing security during the digital transformation era to avoid all threats.

The rapid development of technology is accompanied by an increase in threats, so digital literacy and public awareness need to be emphasized. Public education also contributes to the handling of cyber security [36]. However, data security requires synergy from various parties. The government, the private sector, and the public can work together to improve cyber security in Indonesia in an effort to minimize leaks.

B. Factors Causing Data Leaks in Indonesia

Awareness of the importance of cybersecurity for maintaining national security still needs to be improved by all stakeholders in Indonesia. In line with interviews with BSSN, the main issue in implementing cybersecurity policies is not the challenges themselves, but how these challenges can be overcome collaboratively with all parties.

Many countries such as Malaysia, Singapore, Australia, the United States, and others have taken initial measures in anticipation of cyber security issues, namely cyber security policies [3]. However, the Indonesian government has not been quick enough to respond to this issue. According to interviews with BSSN, this reflects a lack of political will in creating preventive policies, so that new regulations are only created after incidents occur. The lack of political will is also an obstacle because strong and sustained commitment is needed to support the effective implementation of cybersecurity policies. As a result, the regulations that are produced are not in line with the actual needs.

Other factors contributing to data leaks and challenges to strengthening cybersecurity in Indonesia include low cybersecurity awareness, sectoral ego, rapid technological developments, and limited human resources and budgets. The lack of skilled human resources and public understanding of cybersecurity are crucial challenges and concerns that need to be addressed [27]. Interviews with SAFEnet indicate that the government's capacity and readiness to mitigate various risks that may arise from technological developments are considered suboptimal.

C. The Indonesian Government's Efforts to Address Data Leaks and Cyber Security

The era of digital transformation has blurred the boundaries between countries due to technological advances. Interaction has made it easier for everyone to communicate with one another regardless of distance. However, this also poses new risks, particularly related to data security, as information is often shared in cyberspace, so countries around the world are required to ensure national security by implementing cybersecurity policies [3].

Therefore, *political will* is needed from the Indonesian government to address this issue. The Indonesian government's efforts to address data leaks and cyber security are based on seven components of *political will* according to Brinkerhoff [26], as follows:

1. **Government Initiative**
   This component regarding decision-makers must have the initiative to discuss political will itself. Interviews with BSSN indicate that the Indonesian government's first step in forming cybersecurity policy was to establish the National Cyber and Crypto Agency (BSSN) as an effort to improve cybersecurity and defense in Indonesia [30]. This was prompted by the absence of an institution that comprehensively addressed cybersecurity. Previously, this role was limited to the Information Security Directorate at the Ministry of Communication and Information Technology, which only oversaw security aspects of electronic transactions, without implementing technical cybersecurity measures such as

developing algorithms, keys, or encryption. Subsequently, following instructions from President Joko Widodo, cybersecurity responsibilities were consolidated through the merger of the National Cryptography Agency (Lemsaneg), the Information Security Directorate, the Directorate General of Informatics Applications at the Ministry of Communication and Information Technology (Kemenkominfo), and the Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII). This merger aimed to cover all aspects of cybersecurity, including securing, mitigating, and responding to incidents. Since then, authority related to cybersecurity has been handed over to BSSN. However, there is still no specific law regulating cybersecurity and cyber resilience. Even the ITE Law remains limited to electronic transactions, and its revision has not yet accommodated the strategic needs of national cybersecurity. The legal vacuum has prompted BSSN to draft the Cyber Security and Resilience Bill (RUU KKS) and prioritize its discussion by 2025 to ensure comprehensive national cyber protection.

2. **Policy Selection**

State actors choose policies based on considerations and assessments of the potential benefits to be gained. These considerations determine the policy and are considered to be the political will to act. Interviews with BSSN indicate that the Indonesian government has both written and unwritten policies related to cybersecurity. However, the main problem lies in low individual awareness. Many parties feel that "everything is fine," so preventive measures are often neglected, and new steps are taken only after an incident occurs, indicating a lack of political will to make policies. The low level of awareness can be seen from the cases of dangerous APK distribution that remain open to the public despite their known the impact. In addition, government agencies still often use personal gadgets for work, but budget constraints do not allow for the procurement of special devices. Awareness of the importance of information security is also hampered by sectoral ego, for example when BSSN issues warnings about the use of certain systems or technologies, some agencies are reluctant to coordinate because they feel they are higher in the institutional hierarchy. As a result, security measures are often not properly followed. BSSN realizes that security always comes at a high cost and is inversely proportional to convenience. Therefore, the BSSN Regulation No. 8 of 2020 on Information Security Management Systems was issued to require electronic system operators to implement security standards. The three applicable standards are: (1) BSSN standards, (2) ISO 27001 if BSSN standards are not available, and (3) the Information Security Index (KAMI). However, ISO standards are often not used due to their high costs and difficulty in compliance, especially for government agencies, particularly in rural areas. BSSN has also developed minimum standards in Regulation No. 4 of 2023 for SPBE and Regulation No. 8 of 2024 for self-guidance for SMEs (UMKM) as an alternative. Nevertheless, implementation still faces challenges such as budget constraints and limited human resources. These challenges are currently being felt, as audits are conducted on a limited basis, BSSN relies solely on self-reported information from institutions, and direct verification is only conducted if there is sufficient budget.

3. **Stakeholders Mobilisation**

Efforts by government actors to consult, involve, and mobilize all interested parties, including the citizens and the private sector. Interviews with BSSN and Komdigi regarding the collaboration carried out, which is BSSN together with Komdigi and law enforcement agencies (APH) such as the police in handling cybercrimes. Furthermore, cooperation has been established with the Ministry of Law and Human Rights for the formulation of regulations, the Ministry of Finance regarding budgeting, other ministries/agencies, and the private sector. Cyber security is strengthened in a coordinated manner between ministries/agencies and stakeholders with the aim of creating a stronger cyber security ecosystem, reducing the potential for data leaks through technical coordination, regulations, and human resource readiness. BSSN has established a Government CSIRT tasked with handling incidents before, during, and after they occur, including explaining what should and should not be done, such as creating strong passwords, conducting mandatory *PC* monitoring, providing *awareness* before incidents occur, isolating and resetting systems during incidents, and documenting what should be done after incidents to prevent them from recurring in the future. BSSN has also mandated that all ministries/agencies establish a Computer Security Incident Response Team Indonesia (CSIRT) to collaborate with BSSN's Government CSIRT. Every year, BSSN accesses and assesses CSIRTs in K/L. CSIRTs play an important role in maintaining information and technology security within an organization by identifying vulnerabilities, mitigating risks, and restoring systems from cyberattacks or incidents. Furthermore, coordination to improve the competence of human resources is implemented for personnel in ministries/agencies who handle systems but do not have a deep understanding of cybersecurity. Therefore, strengthening is needed in terms of awareness, competence, skills, and networking. In terms of governance, ministries/agencies' compliance with cybersecurity policies has improved compared to before, although awareness and strengthening of culture still need to be improved. Meanwhile, collaboration with the private sector, both state-owned and purely private, and foreign parties, including large companies and start-ups, is aimed at providing guidance from the outset so that they understand the basic principles of cybersecurity. BSSN also collaborates with companies such as

Kaspersky to increase capacity, for example in cybersecurity systems or antivirus development. Although external involvement is not yet widespread due to regulatory and authority limitations, collaboration continues in accordance with the respective roles of each institution. For example, Komdigi focuses on regulation and personal data literacy, while BSSN handles the technical aspects of security. Although their roles are different, their main objective is based on a common issue, namely strengthening national data security. Collaboration with the public is also carried out by facilitating cyber communities to identify vulnerabilities legally, with the hope of reducing information misuse after the program is completed. The VVIP Pilot Project is an example and was conducted from 2022 to 2024 as a trial implementation of the Voluntary Vulnerability Identification and Protection Program (VVIP-Program) involving the public. Collaboration is also carried out with cybersecurity experts to gain in-depth insights and strategies in addressing cyber incidents and threats.

4. **Public Commitment and Resource Allocation**

Public commitment to specific policies, accompanied by the allocation of resources needed to achieve program objectives. Such actions will have a positive impact on political will. Interviews with BSSN indicated that strengthening human resources in the field of cybersecurity still faces challenges, especially in rural areas which often have limited resources and understanding. Central systems connected to rural areas are therefore vulnerable to attacks through weak points. Awareness usually only arises when individuals experience losses such as personal data theft or identity misuse, which is increasingly easy to do with AI technology. As a result, implementation has not been evenly distributed despite capacity building efforts by BSSN and other ministries/agencies. This is because human resources are not placed in accordance with their field of work. For example, after employees attend cybersecurity training, they are sometimes transferred to other units that are not relevant, so that the results of the training are not optimally utilized. In addition, not all employees who handle security systems are civil servants (PNS or P3K), but rather contract employees whose access and integrity are not always guaranteed. Low awareness and integrity in data management also make it difficult to maintain data security. The misuse of access by internal ministry officials in the issue of online gambling is a real risk in this context. Furthermore, budget allocation is important to support the implementation of cybersecurity policies. However, the cybersecurity budget allocation at BSSN is still limited, especially with the national budget efficiency policy. If all ministries and agencies can collaborate and support each other in terms of cybersecurity costs, it will not be a heavy burden. However, in reality, there is still a lot of sectoral ego, where each institution competes to expand its scope of work in order to obtain a larger budget, which actually causes overlapping tasks. Cyber security is a collective responsibility. However, cross-sector collaboration is difficult to achieve. When BSSN was tasked with drafting regulations, ministries and institutions such as Komdigi can provide support in terms of cyber literacy. Despite this, efforts to improve efficiency are taken by maximizing technology for meetings and outreach, aiming to reduce operational costs and ensure that available funds are used effectively and aligned with broader objectives. The estimated losses in the cyber domain by 2025 are projected to reach 14,000 trillion, while the BSSN budget before cuts were approximately 1.5 trillion. This figure is disproportionate if the entire cybersecurity burden is placed on BSSN. Therefore, private sector involvement is also crucial in supporting cybersecurity literacy and awareness.

5. **Credible Sanction**

The implementation of policies with strong political will be reflected through the creation of proper sanctions and strict enforcement. Interviews with BSSN stated that sanctions for cybercrime are regulated in three main regulations, namely the KUHP, the ITE Law, and the PDP Law. However, several provisions in the ITE Law are no longer valid and have been transferred to the new KUHP, which will come into effect in 2023. This indicates a change in the legal approach to cybercrime. There are two categories of cybercrime: cyber as the target of crime, such as hacking, most of which will be regulated in the new KUHP, and cyber as a means of crime, such as online fraud, which is still largely covered by the ITE Law. Although the legal framework is in place, but its implementation still faces major challenges, such as the BPJS data leak case, where the perpetrators and those responsible for criminal liability are still unknown. This shows that regulations and sanctions are not yet fully effective in resolving real cases that should be handled in accordance with applicable provisions. However, the Presidential Regulation regarding the Personal Data Protection Agency under the Personal Data Protection Law, which has the authority to impose sanctions for personal data breaches, has not yet been established [13]. One of the main obstacles lies in the authority of BSSN, which does not have the authority to investigate criminal acts. As a result, the BSSN cannot directly handle cases even if it is at the scene of the incident, because legally the BSSN is not a law enforcement agency (APH) or a civil servant investigator (PPNS). Furthermore, if BSSN accesses an electronic system under attack without following legal procedures, this could be considered interfering with the crime scene (TKP) under criminal procedure law. BSSN can only be involved in legal proceedings if there are two conditions: it is requested by the court as an expert witness or it is officially requested by APH or PPNS. Although BSSN has proposed being granted investigative authority in the 2024 revision of the ITE Law, this proposal has not yet been approved politically or legally, so investigative authority remains with the Police and Komdigi. This situation has slowed down the handling of cyber incidents.

6. **Sustainability of Efforts**
The implementation of policies requires long-term efforts and adequate resource investment to achieve the desired objectives. The results of interviews with BSSN regarding cybersecurity indicate that this is a long-term program, namely requiring comprehensive efforts from the public, organizations, and the government. In 2023, the Indonesian government issued Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management, BSSN Regulation No. 2 of 2024 on Cyber Crisis Management, and BSSN Regulation No. 5 of 2024 concerning the National Cyber Security Action Plan for 2024-2028. The National Cyber Security Strategy and Cyber Crisis Management serve as guidelines for State Institutions and Stakeholders to achieve cyber security strength and capabilities in order to maintain cybersecurity stability. This Presidential Regulation is a proactive effort by the Indonesian government with the main purpose of establishing a comprehensive strategy for maintaining national cyber security, increasing resilience to increasingly complex cyber threats, providing a framework for all stakeholders in dealing with and overcoming cyber incidents, and strengthening coordination among institutions in efforts to maintain cyber security. Other BSSN regulations that have been issued include: BSSN Regulation No. 4 of 2021 on Guidelines for Information Security Management of Electronic-Based Government Systems and Technical Standards and Procedures for the Security of Electronic-Based Government Systems, Regulation of the National Cyber and Cryptography Agency No. 1 of 2024 on Cyber Incident Management, and Regulation of the National Cyber and Cryptography Agency No. 2 of 2024 on Cyber Crisis Management. Additionally, the government's efforts to address the evolving cyber security threats are reflected in Presidential Regulation No. 12 of 2025 on the National Medium-Term Development Plan (RPJMN) for 2025-2029, where cyber security is one of the national priorities 2, and one of the measures to support the achievement of this priority is the Cyber Security and Resilience Bill (RUU KKS), which is based on the increasing national security threats, particularly the number of malware attacks targeting Indonesia. Furthermore, measuring the cybersecurity index in Indonesia in accordance with the Global Cybersecurity Index (GCI) conducted by the International Telecommunication Union (ITU). In the 2024 GCI report, Indonesia is in the highest category of countries based on their commitment to cybersecurity and the "role-modeling" category, which indicates countries with a very strong commitment to cybersecurity.

7. **Learning and Adaptation**
The process of monitoring policies and adapting to situations. Policy makers can observe policies or programs from other countries for adoption in their own countries. Interview results with BSSN regarding monitoring to assess the effectiveness of cybersecurity policies were conducted by examining the implementation of regulations, such as those outlined in BSSN Regulation No. 6 to 9 of 2024, which follow up on Presidential Regulation No. 82 of 2022 on the Protection of Critical Information Infrastructure. Cross-sector activities are also held to ensure the involvement of all stakeholders. However, the effectiveness of some regulations, such as the PDP Law, cannot yet be assessed because the implementing regulations have not been formulated to date. Meanwhile, the ITE Law is considered quite effective as it has been revised twice. Although it is not yet fully capable of accommodating cybersecurity issues, additional regulations are needed based on a review of similar regulations in various countries on cybersecurity, such as China, the United States, Russia, South Korea, Malaysia, Singapore, Japan, and so on. BSSN also actively conducting research, both on how to strengthen existing security perimeters and on deepening the latest technological updates in responding to evolving cyber threats. In strengthening the perimeter, proactive steps are taken by seeking information to learn about the latest cyber attacks and how to detect them. This information is then incorporated into a set of rules or configurations that can be applied across various security perimeters, including firewalls, WAF, EDR, and other security devices. This enables BSSN to prevent and address cyberattacks at an earlier stage. For example, BSSN has container technology virtualization technology, and virtualization technology with bare metal. By studying the characteristics of these technologies, it is possible to learn about their vulnerabilities and help close security gaps through improvements by strengthening perimeter security perimeter devices so that they have more up-to-date rules or configurations. BSSN also conducts research on tools used to complement existing security perimeters to keep them up to date. One example is the creation of File Integrity Monitoring, which can help detect changes in file integrity, enabling early detection of web defacement attempts.

Interviews with BSSN showed that various data leaks reinforce indications of weak cybersecurity in Indonesia in terms of technical aspects, behavior, and regulations. Furthermore, interviews with SAFEnet showed that repeated data leaks are caused by cybersecurity not yet being a priority.

The government's response to cyber incidents has become an issue because many parties are still unwilling to report attacks. The most important thing to know is that the impact of cyberattacks can be fatal, especially if strategic sectors are disrupted. Weak awareness of cyber security has led to data leaks [2]. Protecting data security must be a common concern. In this case, education on cyber security in Indonesia is still minimal, so the government must raise public awareness [36].

The results of interviews with SAFEnet regarding collaboration indicate that government collaboration has not been optimally implemented. This is due to the overlapping authority between BSSN and Komdigi. The PDNS hacking case is a clear example of this lack of coordination. The government has collaborated with ministries/agencies, the public, and the private sector, but implementation has not been optimal.

The authority and limitations of BSSN and Komdigi have prevented the improvement of cybersecurity from being effective. Therefore, in line with Brinkerhoff's *political will*, stakeholders must demonstrate a genuine commitment. The government's commitment to creating a secure cyberspace with clear priorities is key. This commitment can be reflected in budgeting to support digital literacy, provide resources, and implement other improvements to promote cybersecurity.

IV. CONCLUSIONS

Data leaks are a sign that the government has not yet optimally protected national and personal data from cyber threats. Low awareness of cyber security among policy makers has resulted in even greater data leaks. The Indonesian government's political will to address increasingly complex cyber security threats is seen in the establishment of BSSN as the agency responsible for national cyber security. However, addressing these issues by simply forming agency and policies is not enough. Multi-stakeholder cooperation, including the government, the private sector, the public, and foreign countries, is needed to strengthen the government's commitment to maintaining cyber security.

The National Cyber and Encryption Agency (BSSN) and the Ministry of Communication and Digital (Komdigi) provide human resources support to prevent data leaks, but the placement, integrity, and competence of these personnel are not yet adequate or evenly distributed, especially at the regional level. Despite various efforts, data leaks still occur frequently. Issues such as low public awareness of the importance of cybersecurity, weak cybersecurity systems, sectoral egoism within institutions, inadequate public education, and budget constraints are prevalent in Indonesia.

All of these issues can be overcome if policymakers are strongly committed to cybersecurity. Therefore, all stakeholders need to improve security awareness to protect data from leaks, thereby ensuring data security in cyberspace. One step that can be taken by the government is to pass the Cyber Security and Resilience Bill (RUU KKS) to fill the regulatory gap in the field of cybersecurity.

Thus, the protection of state and personal data amid cyber security threats must be guaranteed under a legal framework that is collectively agreed upon and supported by the political will of policymakers in this era of digital transformation. Without strong commitment from the government and policymakers, the implementation of cyber security policies will not be optimal.

REFERENCES

[1] Ridwan, “Implementasi Kebijakan Keamanan Informasi di Pemerintah Provinsi Sulawesi Tengah,” *JIA Fakultas Ilmu Administrasi (FIA)*, vol. 15, no. 2, pp. 1–10, 2018.

[2] S. Ariyaningsih, A. A. Andrianto, A. S. Kusuma, and Rezi, “Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi di Indonesia,” *Justisia: Jurnal Ilmu Hukum*, vol. 1, no. 1, pp. 1–11, 2023.

[3] R. Fitriati, *Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara-Edisi 2, Cet. 1*, 2nd ed. Jakarta: Universitas Pertahanan Indonesia, 2018.

[4] I. N. A. S. Rai, D. Heryadi, and A. Kamaluddin N., “The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber],” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 13, no. 1, pp. 43–66, 2022, doi: 10.22212/jp.v13i1.2641.

[5] N. Olsen, “Blurring the Distinction Between ‘High’ and ‘Low’ Politics in International Relations Theory: Drifting Players in the Logic of Two-Level Games,” *International Relations and Diplomacy*, vol. 5, no. 10, pp. 637–642, 2017, doi: 10.17265/2328-2134/2017.10.005.

[6] BSSN, “Lanskap Keamanan Siber Indonesia 2024,” 2024.

[7] NCSI, “NCSI: Ranking.” [Online]. Available: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

[8] NCSI, “Archived data from 2016-2023.”

[9] A. P. Novita, F. Fatmanegara, F. J. J. Runtuwene, J. T. Samuela, and M. F. Syahbani, “Cyber Security Threats; Analisis dan Mitigasi Resiko Ransomware di Indonesia,” *Jurnal Ilmiah Sistem Informasi*, vol. 3, no. 1, pp. 160–169, 2023, doi: 10.46306/sm.v3i1.91.

[10] Y. Daeng *et al.*, “Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber di Indonesia,” *INNOVATIVE: Journal Of Social Science Research Volume*, vol. 3, no. 6, pp. 1135–1145, 2023.

[11] C. Sorisa, C. L. Kiareni, and J. Parhusip, “Etika Keamanan Siber : Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia,” *Jurnal Sains Student Research*, vol. 2, no. 6, pp. 586–593, 2024.

[12] B. Mudjiyanto, Launa, and A. Leonardi, “Cybercrime, Perlindungan Data Warga Negara, dan Integritas Pemilu,” *Jurnal Oratio Directa*, vol. 5, no. 2, pp. 1058–1085, 2024.

[13] M. K. T. Wibowo, “Tanggung Jawab Komisi Pemilihan Umum Atas Kegagalan Pelindungan Data Pribadi Dalam Pemilihan Umum Tahun 2024,”

Media Hukum Indonesia (MHi), vol. 2, no. 4, pp. 88–95, 2024.

[14] Muh. A. F. Syahril and H. Hasan, "Dampak Kebocoran Data Bjorka pada Kepatuhan Wajib Pajak : Perspektif Akuntansi Keperilakuan," *Jurnal Litigasi Amsir*, pp. 109–115, 2024.

[15] F. S. Putri and A. Suryono, "Langkah Hukum Bagi Peminjam Jasa Pinjaman Pribadi (PINPRI) Atas Kerugian yang Ditimbulkan Akibat Kebocoran Data Pribadi," *Perkara: Jurnal Ilmu Hukum dan Politik*, vol. 2, no. 2, pp. 105–116, 2024.

[16] Kementerian Komunikasi dan Informatika RI, "Persepsi Masyarakat atas Pelindungan Data Pribadi," 2021.

[17] E. Muzairoh, Suharso, D. T. Noviasari, and H. M. Syafingi, "Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital Dalam Prespektif Hak Asasi Manusia," *Borobudur Law and Society Journal (BLASTAL)*, vol. 3, no. 1, pp. 31–36, 2024.

[18] A. F. Apsari *et al.*, "Perlindungan Data Pribadi Pasien Terhadap Serangan Cyber Crime," *Sanskara Hukum dan HAM*, vol. 01, no. 02, pp. 47–53, 2022.

[19] S. Jaelani, "Peran Klasifikasi Serangan Sistem Informasi Dalam Memperkuat Keamanan Nasional dan Memerangi Cyberwarfare," *JICN: Jurnal Intelek dan Cendikiawan Nusantara*, vol. 1, no. 3, pp. 4634–4645, 2024.

[20] I. K. Rahakbauw and I. A. Batubara, "Analisis Potensi Ancaman Siber Pada Bidang Ekonomi di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 7, no. 1, pp. 1–14, 2024, doi: 10.7454/jkskn.v7i1.10089.

[21] I. M. M. Mirza, B. Sujadmiko, and A. Y. Shofura, "Legalitas Cyber Espionage Dalam Hukum Diplomatik (Studi Kasus Penyadapan Kedutaan Besar Australia di Indonesia Pada 2013)," *Res Nullius Law Journal*, vol. 6, no. 2, pp. 154–169, 2024, doi: 10.34010/rnlj.v%vi%i.11678.

[22] B. Simorangkir, T. Legionosuko, and S. D. Waluyo, "Cyber Security Dalam Studi Keamanan Nasional: Politik, Hukum Dan Strategi," *Media Bina Ilmiah*, vol. 17, no. 10, pp. 2409–2414, 2023.

[23] N. Bahtiar, "Darurat Kebocoran Data: Kebutuhan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)*, vol. 2, no. 1, pp. 85–100, 2022.

[24] Sarajevo, *Political Will: a Short Introduction Case Study -Bosnia and Herzegovina*. Friedrich-Ebert-Stiftung (FES), 2015.

[25] J. W. Creswell and J. D. Creswell, *Research Design Qualitative, Quantitative, and Mixed Methods Approaches (Fifth Edition)*. SAGE Publications., 2018.

[26] D. W. Brinkerhoff, "Unpacking The Concept of Political Will to Confront Corruption," 2010.

[27] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of The Art, Challenges and Future Directions," *Cyber Security and Applications*, vol. 2, 2024, doi: 10.1016/j.csa.2023.100031.

[28] A. Yulianto, "Cybersecurity Policy and Its Implementation in Indonesia," *Law Research Review Quarterly*, vol. 7, no. 1, pp. 69–82, 2021, doi: 10.15294/lrrq.v7i1.43191.

[29] Group-IB, "High-Tech Crime Trends Report 2025." [Online]. Available: https://www.group-ib.com/landing/high-tech-crime-trends-2025/

[30] S. M. Sutra and A. Haryanto, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal*, vol. 7, no. 1, pp. 56–69, 2023, doi: 10.34010/gpsjournal.v7i1.8141.

[31] A. F. Yamin, A. Rachmawati, R. A. Pratama, and J. K. Wijaya, "Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi," *Meraja Journal*, vol. 7, no. 2, pp. 138–155, 2024.

[32] BSSN, "Lanskap Keamanan Siber Indonesia 2023," 2023.

[33] H. C. Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 10, no. 2, pp. 113–128, 2019, doi: 10.22212/jp.v10i2.1447.

[34] I. T. Islamy, S. T. Agatha, R. Ameron, B. H. Fuad, and N. A. Rakhmawati, "Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi," *Jurnal Teknologi Informasi dan Pendidikan*, vol. 11, no. 2, pp. 21–28, 2018.

[35] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 13, no. 2, pp. 222–238, 2023, doi: 10.22212/jp.v13i2.3299.

[36] Y. C. Mahendra and N. K. D. S. A. Pinatih, "Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia," *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, vol. 6, no. 4, pp. 1941–1949, 2023.