Submitted	Review Process	Revised	Accepted	Published
17-01-2023	11-02 s/d 18-05-2023	22-05-2023	31-05-2023	30-06-2023

Jurnal Studi Sosial dan Politik. Vol. 7, No. 1, June 30, 2023 (50-62)
ISSN: 2597-8756
E-ISSN: 2597-8764

Jurnal Studi Sosial dan Politik Published by FISIP, Universitas Islam Negeri Raden Fatah Palembang

Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era

Futri Bela Fransiska
Faculty of Social and Political Sciences, Universitas Indonesia
Email: Futri.bela@ui.ac.id

Fredy BL. Tobing
Faculty of Social and Political Sciences, Universitas Indonesia
Email: Fredyblt@ui.ac.id

Abstract

Indonesia, a densely populated country with many internet users, witnesses the daily reliance on internet activities. With the convergence of personal and state data in the cyberspace domain, driven by the rapid development and modernization of information and communication technology, ensuring the security of this interconnected realm becomes paramount. The global expansion of the internet, accompanied by a surge in users each year, has eliminated boundaries and created an incessant presence within cyberspace. Consequently, countries must guarantee the protection of information and data in this domain, particularly considering the rising cybercrime incidents, which have further intensified following the COVID-19 pandemic. The increased reliance on the internet has compelled nations and individuals to prioritize cybersecurity and leverage its potential to meet evolving needs. The objective of this research is to assess Indonesia's readiness in confronting this new dimension, as it holds the potential to impact the economy, politics, and state sovereignty. With numerous instances of cross-border cybercrime occurring in Indonesia, the study utilizes a qualitative research methodology, incorporating both secondary and primary data collection. The findings reveal that Indonesia is actively working towards strengthening its cybersecurity through bilateral, multilateral, and cyber diplomacy collaborations with various relevant agencies such as the Ministry of Foreign Affairs and the Ministry of Defence, as well as the BSSN (National Cyber and Encryption Agency).

Keywords: Information Technology, Cyber-Crime, Cyber-Space, Cyber-Security, Institutional, Indonesia

Abstrak

Indonesia, sebuah negara yang padat penduduk dengan banyak pengguna internet, menyaksikan ketergantungan harian pada aktivitas internet. Dengan penyatuan data pribadi dan data negara dalam ranah dunia maya (cyberspace), didorong oleh perkembangan dan modernisasi yang pesat dalam teknologi informasi dan komunikasi, memastikan keamanan dari wilayah terhubung ini menjadi sangat penting. Perluasan global internet, yang diikuti oleh peningkatan jumlah pengguna setiap tahunnya, telah menghilangkan batasan dan menciptakan kehadiran yang tidak henti di dalam dunia maya (cyberspace). Oleh karena itu, negara-negara harus menjamin perlindungan informasi dan data di ranah ini, terutama mengingat meningkatnya kejadian kejahatan siber yang semakin intensif setelah pandemi COVID-19. Ketergantungan yang meningkat pada internet telah mendorong negara-negara dan individu untuk memberikan prioritas pada keamanan cyber dan memanfaatkan potensinya untuk memenuhi kebutuhan yang terus berkembang. Tujuan dari penelitian ini adalah untuk mengevaluasi kesiapan Indonesia dalam menghadapi dimensi baru ini, karena memiliki potensi untuk berdampak pada ekonomi, politik, dan kedaulatan negara. Dengan banyaknya kasus kejahatan siber lintas batas yang terjadi di Indonesia, penelitian ini menggunakan metodologi penelitian kualitatif yang melibatkan pengumpulan data sekunder dan primer. Temuan penelitian menunjukkan bahwa Indonesia aktif dalam memperkuat keamanan cyber melalui kerjasama bilateral, multilateral, dan diplomasi cyber dengan berbagai lembaga terkait seperti Kementerian Luar Negeri, Kementerian Pertahanan, serta BSSN (Badan Siber dan Sandi Negara).

Kata Kunci: Teknologi Informasi, Kejahatan Siber, Dunia Maya (Cyberspace), Keamanan Cyber, Institusional, Indonesia

INTRODUCTION

The development of information and communication technology continues to advance, becoming more sophisticated and bringing significant benefits to help every global citizen. In this development, it is not only one government or private group that utilizes the evaluation of this technology, but it has also facilitated all global citizens to connect with individuals, groups, NGOs, and countries (Rahmadany & Ahmad, 2021). Additionally, it provides many benefits for each user and progress in modern conditions that are proportional to the increase in the number of internet and cyber users, which impacts international relations. Every data owned by a country or citizen that is transmitted through the internet is potentially threatened in terms of confidentiality or free dissemination. In this context, governments and non-state actors must make efforts to secure their data and activities in the cyber world (Buchan, 2016). Therefore, the role of the state is needed to guarantee and protect data confidentiality in the cyber world (Weber, 2010).

The cyber world has become a new world not only for business and social activities but also functions as an environment for crime, hacking, and terrorism. Everyone connected to the cyber world faces potential security threats within that virtual world. The cyber world is a different world characterized by the ability of virtual presence. The internet has become an essential need in society, providing not only information and entertainment but also a sense of security and comfort in the cyber world. Almost every individual uses the internet for various

needs, and around 60% of the world's population are internet users in the virtual world (Westcott, 2008). Therefore, cybercrime takes various forms, including cyber fraud, such as scams that provide false information to gain profits; information theft, also known as phishing; carding, which involves using other people's debit or credit card data for criminal purposes; sharing login information, where perpetrators exploit stolen data to gain unauthorized access to other people's accounts; and social engineering techniques, which manipulate victims into unknowingly providing personal information, enabling perpetrators to easily influence them. On the other hand, internet advancements have facilitated online transactions and created a rapidly growing online market, making security a crucial concern for the sustainability of e-commerce worldwide.

According to Legionosuko et al. (2019), the concept of war has undergone a paradigm shift, extending beyond traditional armed conflicts to include trade wars, information wars, cyber warfare, proxy wars, and other forms of asymmetric warfare. Babys (2021) explains that cyber warfare significantly differs from conventional warfare as it can be conducted by both state and non-state actors in the limitless and timeless realm of the virtual world. Cyber warfare encompasses various operational forms, such as hacking, attacks, alteration, sabotage, interception, disruption, manipulation, theft, intervention, exposure, and overthrow. These developments in the cyber world have resulted in cybercrime, which, in a broader scope, can pose threats to state sovereignty, territorial integrity, and national security. Chotimah et al. (2019) acknowledges that cyber security threats are not only recognized as technical computer security issues but also encompass ideological, political, economic, social, cultural, and national security aspects. The U.S. Department of Defence identifies the increasing frequency of cyber-attacks in the virtual world as one of the most significant threats to national security. Targeted cyber-attacks can compromise critical infrastructure such as transportation systems, energy networks, telecommunications systems, and the financial sector. Countries that are unable to defend and protect their cyber infrastructure are vulnerable to attacks from malicious actors. International cooperation and public-private sector collaboration in cyber protection are necessary to address these threats.

Security and defence are fundamental in safeguarding national sovereignty. National defence and security aim to protect and defend the country on land, sea, and air. However, the paradigm has shifted with the development of information and telecommunications technology, where the virtual world has become borderless and timeless. The virtual world has emerged as a domain of defence and security due to its vulnerability, giving rise to cyber warfare (Hilmy & Azmi, 2021). Cybersecurity has become a primary concern in international relations for governments and the private sector, leading to enhanced security measures and multilateral cooperation to address cyber threats. In the concept of warfare in the virtual world, actors cannot be limited to a specific group such as government or state actors. Actors in the cyber world can be individuals, hacker groups exploiting data, non-governmental organizations, terrorist networks, or private sector companies driven by various motives including competition (Pearlman & Cunningham, 2012; Rohali & Yumitro, 2022).

The adoption of digital technology has rapidly increased globally, including at the national level, including in Indonesia. In Indonesia, internet users consist of various groups, including the government, students, businesses, and employees. Indonesia has a significant number of internet users according to BPS data from the 2021 (Marhaeni, 2022). In 2021, 62.10% of the Indonesian population accessed the internet, indicating ongoing technological and informational developments. This encourages the disclosure of information, acceptance, and societal adaptation to the new world in the cyber realm, enabling people to connect and

obtain useful information and data (Marhaeni, 2022). Therefore, Indonesia needs to make efforts to secure the cyber world as weak defence and security mechanisms in the cyber realm can create vulnerabilities for the country and other actors to interfere in Indonesia's sovereignty (Widarda, 2020). Such interventions can include state information theft, propaganda, terrorism, eavesdropping, the spread of hoaxes or false information, and potential conflicts (Arisanty et all., 2022). Attacks on vital information systems such as government websites, military networks, or national defence systems are also possible. The COVID-19 pandemic in 2020 has led to an increase in internet users in Indonesia, proportionally increasing cyber-attacks in the country, as reported by BSSN (National Encryption and Cyber Agency). This poses a significant threat to national defence and security. Without clear protection concepts, cyber-attacks in Indonesia will continue to increase.

According to BSSN data, in the period from January to April 2020 alone, there were approximately 80 million cyber-attack incidents in Indonesia, indicating a considerable number in a relatively short period. The absence of adequate protection, laws, and policies can ultimately endanger the security and defence of the Republic of Indonesia. With the extensive development of the virtual world, it has become a domain that requires protection. The Indonesian National Defence Law, Law Number 3 of 2002, recognizes that threats to the national defence system can include both military and non-military domains, with cybercrime being a particular threat to national defence. While the cyber world provides convenience and comfort for internet users in Indonesia, it also poses potential threats. In 2018, Indonesia ranked fifth as the most frequently targeted cyber-attack destination in the Asia-Pacific region, emphasizing the need for Indonesia to protect its infrastructure and technological facilities on the internet (Chotimah, 2019). Based on a report on the state of the internet in 2013, Indonesia ranked second in the world as a country with cybercriminals (Afiah, 2018). Therefore, the National Data Security Index predicts that Indonesia will rank 83rd in 2021 (NCSI, 2023).

The Indonesian government has increased efforts in cybersecurity through various measures. The National Encryption and Cyber Agency (BSSN) is the institution responsible for protecting the country's cybersecurity. BSSN has launched various programs, such as human resource development programs, cybersecurity training, and cooperation with national and international institutions to build capabilities in protecting Indonesia's cyber infrastructure. Additionally, BSSN collaborates with the private sector and NGOs in joint efforts to enhance cybersecurity. Private companies in Indonesia are also expected to increase awareness of cybersecurity and implement appropriate security practices in their infrastructure. Furthermore, the protection of personal data has become an important focus with the enactment of the Personal Data Protection Law (PDP Law) in 2019, aiming to protect individuals' personal data and ensure the security and privacy of data in activities involving personal data processing. Despite efforts being made, cybersecurity challenges persist and continue to evolve with technological advancements. Cooperation and collaboration between the government, private sector, and civil society are necessary in efforts to protect cyber infrastructure, raise awareness of cybersecurity, and develop capabilities to face evolving threats in the virtual world (Bechara & Schuch, 2020; Carr, 2016).

This paper is divided into three parts to provide a comprehensive analysis of the topic. First, it focuses on the development of technology and its relationship to cyber-attacks. It explores how advancements in technology, particularly in the field of information and telecommunications, have created new opportunities for cyber threats. The discussion delves into the evolving nature of cyber-attacks, including the emergence of sophisticated hacking techniques, data breaches, and the exploitation of vulnerabilities in digital systems. The rapid

expansion of the virtual world has made cyber-attacks a pressing concern for governments, organizations, and individuals worldwide. Second, it examines the specific issues related to Indonesia's cyber space. It highlights the increasing adoption of digital technology in Indonesia and the subsequent rise in internet users. This section discusses the country's susceptibility to cyber threats due to its expanding online presence. It explores the challenges faced by Indonesia in terms of cyber-attacks, such as the targeting of government websites, the potential for data theft, and the spread of misinformation. The discussion also addresses the need for enhanced cybersecurity measures and increased awareness among Indonesian internet users to mitigate these threats. Third, it focuses on the strategies adopted by Indonesia to counter cyber space attacks. It discusses the efforts of the Indonesian government, particularly through the National Encryption and Cyber Agency (BSSN), to strengthen cybersecurity measures. This section highlights various initiatives, such as human resource development programs, cybersecurity training, and collaborations with national and international institutions. It also emphasizes the importance of public-private partnerships and the implementation of robust cybersecurity practices by private companies operating in Indonesia. The discussion underscores the significance of a comprehensive and coordinated approach to cybersecurity, encompassing both preventive measures and incident response strategies. Therefore, this research provides a comprehensive examination of the interplay between technology development, cyber-attacks, Indonesia's cyber space issues, and the country's strategies to combat these threats. By delving into these three interconnected areas, the research offers insights into the evolving cybersecurity landscape and the measures necessary to protect Indonesia's digital infrastructure.

RESEARCH METHOD

This research employs qualitative research. Following the definition by Lawrence Neuman (2014), qualitative research focuses on the exploration, understanding, and analysis of data. In this study, an exploratory qualitative research approach is used to investigate the cyber security of cyberspace in Indonesia and the concept of institutional cooperation. The unit of analysis includes relevant government agencies, institutions, and the country itself, aligning with the research's focal point. Secondary data is utilized in this paper through literature studies. Literature studies involve the compilation and summary of articles from journals, books, and other documents. Additionally, primary data is gathered through interviews conducted with staff members at BSSN (the Indonesian National Cryptography Agency), and by referring to documents from the ASEAN Regional Forum and ASEAN itself. The data sources for this study encompass international cyber threat cases, cyber threats in Indonesia affecting both the government and society, and relevant research data and cases from 2008 to 2021.

Various government institutions in Indonesia play a crucial role in securing cyberspace. These include the Ministry of Foreign Affairs, responsible for cyber diplomacy; the Indonesian National Army and the Ministry of Defence, focusing on cyber defence; the Ministry of Communications and Informatics; and the Republic of Indonesia Police. Additionally, the formation of BSSN in 2017 was specifically aimed at securing cyberspace in Indonesia.

Qualitative data, as outlined by Creswell et al. (2007), can take various forms such as photographs, maps, open interviews, observations, and documents. The data collected in this study falls into two main categories: field research, encompassing ethnography, participant observation, in-depth interviews, and historical-comparative research. Through a constructivist approach, this study aims to analyse the Indonesian government's response to potential cyber threats and elucidate Indonesia's efforts and cooperation in ensuring cyber security in the current era.

RESULT AND DISCUSSION

Political development is an important aspect of progress and modernity in a country. With modernity comes interconnectedness, transcending time, and borders. Developing countries, such as Indonesia, strive to catch up in this regard. President Jokowi has stated that Indonesia will embark on the path towards Industry 4.0, which entails utilizing technology in production chains. This development raises speculation among various stakeholders, including political elites and industry players. The definition of Industry 4.0 (Klingenberg et al., 2021; Zheng et al., 2021), indicates that Indonesia will undergo radical changes in processes and industrial development, leading to new challenges. One of these challenges is data security, which raises general concerns among the Indonesian population (Margiansyah, 2020).

In the 21st century, our daily lives are deeply connected to cyberspace (Sen, 2000). Cyberspace has become a necessity, and the confidentiality of personal data within it is threatened. Consequently, a sense of security has become a fundamental need for individuals worldwide who are connected to cyberspace. Threats to nations and states have evolved into multidimensional challenges, encompassing ideological, sovereignty, political, economic, and socio-cultural issues. Additionally, security concerns extend to international crimes, including illegal fishing, terrorism, radicalism, extremist media influencing violence (Panjaitan, 2020), drug smuggling, human trafficking, illegal immigration, piracy, and environmental destruction (Emmers, 2003). These threats fall into two categories: military threats and non-military threats, both of which have become crucial topics on Indonesia's foreign policy agenda due to their impact on sovereignty (Jasparro & Taylor, 2008).

Cyberspace is a highly dynamic and complex realm. The entire cybersecurity problem revolves around data availability in cyberspace. The confidentiality of private data and personal actions is at risk. Cybercrime and cybercriminals pose a significant danger. Cybercrime involves criminal activities using computers and computer networks within cyberspace or through other information and communication technology media. Perpetrators employ viruses, malware, and distributed denial of service (DDoS) attacks via various channels. Hacked email accounts can be exploited for crimes like fraud, aligning with the hacker's main objective (McGuire & Dowling, 2013). Cyber warfare, as defined by Clarke & Knake, (2014), refers to an act where one nation penetrates another's computer or network to cause damage or disruption (Zotti, 2011). Significant cyberattacks have occurred since 1998, including conflicts between India and Pakistan over Kashmir, where both sides developed cyber militias to conduct attacks on each other (Caplan, 2013; Syed & Ahmed, 2021).

Cybersecurity and political security intersect. In Indonesia, national cybersecurity is considered inadequately managed and lacks proper integration. This issue stems from the absence of a specific organization dedicated to national cybersecurity. According to Frost & Sullivan (2017), cybercrime has caused Indonesia a deficit of approximately 34.2 billion USD (Shafira, 2021). Hacking incidents have targeted several sites known for their robust cybersecurity, including the hacking of former President Susilo Bambang Yudhoyono's personal phone and numerous cases of mass media and government organization hacks, as well as online fraud cases are also prevalent.

Cybersecurity has become a national priority, particularly in developing countries (Kim, 2014). The increasing utilization of information and communication technology, especially during the COVID-19 pandemic, affects various aspects such as government and state affairs, economy and politics, education, national defense, and healthcare (Sukarno & Saleh, 2022). In 2017, the President of Indonesia established the BSSN (National Cyber and Encryption Agency) as a government institution responsible for handling national cybersecurity issues and ensuring prevention and mitigation of threats from cyberspace. The BSSN underwent a transformation process to become a credible institution and a pillar of cybersecurity in

Indonesia. It plays a strategic role in integrating and coordinating cybersecurity systems at the national, regional, and international levels (Wibowo et al., 2020).

According to BSSN data, four of the largest e-commerce platforms in Indonesia have experienced data breaches or leaks, which can be carried out by companies or individuals. For example, Tokopedia reported a data leak of 91 million users. The international internet security company, Eset, operating in Indonesia, faces approximately 1.225 billion cyberattacks every day. As per the Ministry of Information and Communication Republic Indonesia, internet users in Indonesia during the second quarter of 2019-2020 reached 196.7 million, divided into four categories: Google Balloon internet usage, satellite usage, Wi-Fi usage, and ISP (Internet Service Provider) usage.

Indonesia Cyber-Spaces Issues

Indonesia, with its high population and extensive internet usage, is vulnerable to risks and cyber threats. This poses a significant danger to the country and its citizens, especially considering their high dependence on communication and information technology. The advancement of technology has led to increasingly sophisticated and complex threats in cyberspace. The level of dependence and application of technology directly correlates with the risks associated with information and communication technology. While conflicts were previously confined to traditional weapons like firearms and bombs, cyber threats have emerged, such as information theft or access colonization for specific purposes. When perpetrators bridge international borders to steal and dismantle confidential data, these crimes become categorized as international threats. State and non-government actors can carry out such crimes, aiming to disrupt activities. Cyberattacks often take the form of malware, cybercrime, cyber threats, or computer misuse. These criminal activities can occur anywhere, particularly in countries with low awareness and high internet usage, providing opportunities for internet crimes like hacking.

Indonesia has experienced numerous cyberattacks, including incidents like wiretapping by Australia against the Indonesian government and espionage on the personal phone of former President Susilo Bambang Yudhoyono and several Indonesian ministers. While Indonesia's positive law does not specifically regulate espionage actions, the Australian Intelligence collected data on the phone numbers of Indonesian officials during the Climate Change Conference in Bali.

During the 2009 election of President Susilo Bambang Yudhoyono, Australian Intelligence staff wiretapped the cell phones of Mrs. Any Yudhoyono, the Ministry of Economy Hatta Rajasa, and the Minister of Defense, General Djoko. The United States has also been involved in surveillance activities, including bugging European countries and several Southeast Asian countries. These incidents led President SBY to temporarily withdraw the Indonesian Ambassador from Canberra and cancel military cooperation and people smuggling policies. Espionage between countries is not a new issue in the intelligence community, and it is generally not brought to the International Court of Justice. Globalization has facilitated information technology waves, blurring the sovereignty boundaries of countries.

Indonesia is considered a prime target for hackers and ranks 84th in the National Cyber Security Index (NCSI) with a cyber security digital development score of -7.88 (NCSI, National Cyber Security Index, 2022). The number of internet users in Indonesia continues to rise, and by 2021, Indonesia is projected to become the fourth-largest country in terms of internet users. However, the development of internet users in Indonesia has not been matched by the level of cyber security, resulting in a weak cyber security infrastructure, and encouraging cybercrime in various domains, including civil, strategic, and military sectors.

Akhmad Muqowam, Chairman of Committee I at the Indonesian Regional Representative Council (DPD), revealed that Indonesia ranks second in the world for cybercrime, specifically in hacking through cyberspace. This cybercrime spans various fields, such as e-commerce and banking, each with different levels of international security standards. Improving security requires better coordination among users. Additionally, Indonesia was also the second country affected by the Stuxnet worm attack in 2010, which infected around 60,000 computers worldwide. This sophisticated cyber worm program aimed to gain control over remote systems in a semi-autonomous manner. The attack occurred in several countries, including India, China, Azerbaijan, Finland, South Korea, Germany, the United Kingdom, Iran, Australia, the United States, and Malaysia. While viruses continue to spread and infect computer systems through the internet, their destructive power has been limited by the availability of effective antidotes (Farwell & Rohozinski, 2011).

Indonesia Strategy in Cyber Space

After experiencing various cases that have disturbed the government and society, such as personal data breaches, Indonesia needs to take an active stance against cybercrimes and enhance domestic cyber security. The country already has a system and strategies in place through government agencies. One of the reasons for the increasing cybercrime and cyberattacks in Indonesia is the recorded over 1.6 billion cases or traffic anomalies in cyberspace in 2021, as reported by BSSN. The issue of cyber security in Indonesia requires attention from the government, and it began with the policy issued in 2007, specifically the Minister of Communication and Information Technology Regulation No. 26 PER/M.Kominfo/5/2007 concerning the Security of Use of Internet Protocol-Based Telecommunication Networks (Yulianto, 2021).

Indonesia has demonstrated a strong commitment to cyberspace and continues to contribute to digital protection in collaboration with diplomatic efforts. Through its membership and administration role in the International Telecommunication Union (ITU) from 2008 to 2013, Indonesia promoted shared values and standards in cyberspace globally. The country actively supports the values within the organization, recognizing its significant role as an ITU member (Iswardhana, 2021). Indonesia also engages in international cooperation related to cyberspace, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), which is a cyber security alliance supported by the United Nations. Member countries actively participate in IMPACT programs to maintain global stability in the face of cyber threats (Rai et al., 2022).

Indonesia continues to strengthen its capabilities in securing cyberspace to safeguard its sovereignty. Initiatives such as the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) and the National Cyber and Crypto Agency (BSSN) play vital roles in coordinating and cooperating with other institutions related to cyber interests in Indonesia. These institutions collaborate with various entities, including the Ministry of Foreign Affairs for cyber diplomacy, the police for cybercrime, the Indonesia National Army and the Ministry of Defence for cyber defence, and the Ministry of Communications and Informatics, among others.

According to data from BSSN, there were 88,414,296 cyberattacks reported from January to April in 2020. Most of these attacks involved trojan viruses (56%) and illegal information gathering activities (43%), with site application attacks accounting for the remaining 1%. By the end of 2020, the number of cyberattacks increased to 423,244,053. In 2017, a global cyberattack known as the WanaCrypt0r 2.0 spread rapidly and infected countries worldwide. The Indonesian government, through BSSN, actively conducts socialization and training both online and offline to enhance human capabilities in addressing global challenges.

Collaborative efforts between BSSN and stakeholders are prioritized in taking action (Sa'diyah & Vinata, 2016).

BSSN provides certifications for individuals involved in cyber security activities. Through the Professional Certification Institute, BSSN collaborates to identify the needs in the business world. Additionally, BSSN engages in standardization activities with various ministries, including the Ministry of Manpower of the Republic of Indonesia, the Ministry of Industry, and BSSN itself. The occupational map developed by BSSN includes strategies such as implementing "The Unified Kill Chain" framework and dividing the Occupational map based on the Attack (Before-During-After) phase. Furthermore, BSSN has established 30 occupations in the Indonesian National Qualifications Framework, aiming to build effective career paths and expertise based on required certifications.

These efforts encourage Indonesia to prioritize cyber security and continuously improve its performance and international cooperation. BSSN, as an implementing agency for Indonesia's cyber diplomacy, collaborates bilaterally with several countries, including Australia, the Kingdom of the Netherlands, and the United States. In the field of cyber diplomacy, BSSN works in synergy with the Ministry of Foreign Affairs to safeguard national interests in the transnational network of the internet, considering the complex and cross-country nature of cyber threats (Narindra, 2021).

Diplomacy plays a crucial role in achieving a country's national interests in international relations. Cyberspace, with its unique characteristics, frames diplomatic engagement among stakeholders (Balleste & Kulesza, 2013; Barrinha & Renard, 2017). Indonesia's cooperation in cyber and digital security extends to Australia, with a focus on the digital economy. The collaboration aims to advance cooperation and capacity building in areas such as the development of a national cyberspace strategy, national incident management capabilities, capacity building, and cooperation in cybercrime prevention (Rosy, 2020). An MoU between BSSN Indonesia and Australia was signed on September 8, 2021, encompassing various aspects, including Cyber and Emerging Cyber Technology Cooperation. Indonesia, acting as a balancer, actively contributes to the partnership, particularly in areas related to the digital economy, cybercrime, capacity building, and information sharing (Aprilianti & Dina, 2021).

As an active member of ASEAN, Indonesia engages in multilateral cooperation in the region. ASEAN serves as a platform for sharing regional perspectives, including addressing the threats of cyber security. The stability of cyberspace is crucial for economic progress, especially in the era of digital economy. The ASEAN Cybersecurity Cooperation Strategy draft emphasizes building strong cooperation among Computer Emergency Response Teams (CERTs) and capacity building in the Asian region. Indonesia also participates in the ASEAN Regional Forum (ARF), which has been discussing cyber threats since 2006. At the 19th ARF forum in 2012, the foreign ministers adopted the Statement of Cooperation on Ensuring Cyber Security, highlighting the importance of cyber security in the context of the ASEAN Political-Security Community (ASEAN, 2020)s. Indonesia actively contributes to the ITU, an organization at the forefront of promoting shared values and standards in cyberspace for positive use. Given the significance of cyberspace in reshaping the international economic and political environment, Indonesia actively engages in various cyber forums (Mukhtar & Firdaus, 2020). Multilateral agreements, such as TELMIN and CERTS, provide platforms for discussions on cyber issues and the threats of cyberattacks (Iswardhana, 2021).

CONCLUSION

One of the most significant wiretapping incidents in Indonesian history occurred in 2009 when Australia wiretapped the cell phone of the President, resulting in strained relations between Indonesia and Australia. This incident led President SBY to temporarily withdraw the Indonesian Ambassador from Canberra and cancel several cooperation agreements. The emergence of cyberspace has introduced a new dimension to information security, especially in the aftermath of the COVID-19 pandemic. The development of the cyber world in each country also impacts the international political arena, as seen in instances where world leaders are targeted by cyberattacks. The increasing frequency of cyberattacks necessitates Indonesia to enhance its cyber security measures, considering its status as a large country with a high population and a growing number of internet users each year. In this era of cyber diplomacy, Indonesia needs to put forth more efforts through relevant ministries in collaboration with other countries, both in bilateral and multilateral settings.

The Ministry of Foreign Affairs, Ministry of Defense, Ministry of Communication, and Informatics, and the National Cyber and Crypto Agency (BSSN) coordinate tasks among various institutions and carry out their respective duties to ensure cyber security in Indonesia. Establishing partnerships through bilateral, multilateral, and regional forums is crucial, as building cybersecurity is a complex process that requires cooperation with other nations. Security must be integrated among relevant institutions and regulated by the government. Indonesia continues to work diligently to secure its country and sovereignty in cyberspace. As a nation with one of the highest numbers of internet users globally, Indonesia must prioritize ensuring cybersecurity at both the national and global levels.

REFERENCES

Afiah, N. (2018). Pengaruh Keamanan, Reputasi Dan Pengalaman Terhadap Trust Pengguna Internet Untuk Bertransaksi Secara Online. *JEKPEND: Jurnal Ekonomi Dan Pendidikan*, *1*(2), 58. https://doi.org/10.26858/jekpend.v1i2.7256

Aprilianti, I., & Dina, S. A. (2021). *Co-regulating the Indonesian Digital Economy*. *Policy Paper no. 30*, 1–40.

Arisanty, M., Febrina, N., Wiradharma, G., & Ginting, E. (2022). Social Media Users in Receiving and Sharing Hoax Information: Overview from Motivation Level. *Jurnal Studi Sosial Dan Politik*, *6*(1), 80–100. https://doi.org/https://doi.org/10.19109/jssp.v6i1.12238

ASEAN. (2020). *ASEAN Cybersecurity Cooperation Strategy (2021-2025)*. 1–14. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Balleste, R., & Kulesza, J. (2013). *Fordham Intellectual Property , Media and Entertainment Law Journal Signs and Portents in Cyberspace : The Rise of Jus Internet as New Order in International Law Signs and Portents in Cyberspace : The Rise of Jus Internet as New Order in International Law*. *23*(4).

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges.

Journal of Financial Crime, *28*(2), 359–374. https://doi.org/10.1108/JFC-07-2020-0149

Buchan, R. (2016). Cyberspace, non-state actors and the obligation to prevent transboundary harm. *Journal of Conflict and Security Law*, *21*(3), 429–453.

Caplan, N. (2013). Cyber War: the Challenge to National Security. *Global Security Studies*, *4*(1).

Carr, M. (2016). Public – private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. (2019). Penerapan Military Confi dence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. *Jurnal Ketahanan Nasional*, *25*(3), 331. https://doi.org/10.22146/jkn.50344

Clarke, R. A., & Knake, R. K. (2014). *Cyber war. Old Saybrook: Tantor Media, Incorporated*. Old Saybrook: Tantor Media, Incorporated.

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and Implementation. *The Counseling Psychologist*, *35*(2), 236–264. https://doi.org/10.1177/0011000006287390

Emmers, R. (2003). The Threat of Transnational Crime in Southeast Asia: Drug Trafficking, Human Smuggling and Trafficking and Sea Piracy. *Revista UNISCI*, *2*, 1–11. http://www.unisci.es/the-threat-from-transnational-crime-in-southeast-asia-drug-trafficking-human-smuggling-and-trafficking-and-sea-piracy/

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Frost & Sullivan. (2017). *Cyber Security in the Era of Industrial IoT*. 1–27.

Hilmy. Muhammad Irfan &, & Azmi, R. H. N. (2021). Konstruksi Pertahanan dan Keamanan Negara terhadap Perlindungan Data dalam Cyberspace untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lemhannas RI*, *9*(1), 114–124. https://doi.org/10.55960/jlri.v9i1.381

Iswardhana, M. R. (2021). Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia. *Journal of Islamic World and Politics*, *5*(2), 343–367. https://doi.org/10.18196/jiwp.v5i2.12242

Jasparro, C., & Taylor, J. (2008). Climate change and regional vulnerability to transnational security threats in Southeast Asia. *Geopolitics*, *13*(2), 232–256. https://doi.org/10.1080/14650040801991480

Kim, S. (2014). Cyber Security and Middle Power Diplomacy. *The Korean Journal of International Studies*, *12*(2), 323. https://doi.org/10.14731/kjis.2014.12.12.2.323

Klingenberg, C. O., Borges, M. A. V., & Antunes, J. A. V. (2021). Industry 4.0 as a data-driven paradigm: a systematic literature review on technologies. *Journal of Manufacturing Technology Management*, *32*(3), 570–592. https://doi.org/10.1108/JMTM-09-2018-0325

Lawrence Neuman, W. (2014). *Social Research Methods: Qualitative and Quantitative Approaches W. Lawrence Neuman*.

Legionosuko, T., Madjid, M. A., Asmoro, N., & Samudro, E. G. (2019). Posisi dan Strategi Indonesia dalam Menghadapi Perubahan Iklim guna Mendukung Ketahanan Nasional. *Jurnal Ketahanan Nasional*, *25*(3), 295. https://doi.org/10.22146/jkn.50907

Margiansyah, D. (2020). Revisiting Indonesia's economic diplomacy in the age of disruption: Towards digital economy and innovation diplomacy. *Journal of ASEAN Studies*, *8*(1), 15–39. https://doi.org/10.21512/jas.v8i1.6433

Marhaeni, H. (2022). *Direktorat Statistik Keuangan Teknologi Informasi dan Pariwisata Indonesia 2022*. Https://Ppid.Bps.Go.Id/. https://ppid.bps.go.id/upload/doc/LAKIN_Direktorat_Statistik_Keuangan___TI__dan_Pariwisata_2022_1683604348.pdf

McGuire, M., & Dowling, S. (2013). A targeted attack occurs when the organisation is of specific interest to the attacker, who plans the digital offensive many months before it is launched. In *Home Office Research Report 75* (Issue October). London, England, United Kingdom

Mukhtar, A., & Firdaus, A. (2020). ASEAN Community and Prospects for the Development of UIN Raden Fatah Palembang. *Jurnal Studi Sosial Dan Politik*, *4*(2), 109–121. https://doi.org/https://doi.org/10.19109/jssp.v4i2.6771

Narindra, K. S. (2021). Keamanan dan Ancaman Cyber Bagi Sektor Privat dan Industry Militer Di Era 4.0. *Jurnal Diplomasi Pertahanan*, *7*(1), 36–55. https://doi.org/10.33172/jdp.v7i1.675

NCSI. (2023). *National Cyber Security Index*. Https://Ncsi.Ega.Ee/. https://ncsi.ega.ee/ncsi-index/?order=rank

Panjaitan, S. N. (2020). Transformation of Radicalism Discourse into Extremist Violence (Analysis of News on the Handling of Radical Movements in Indonesia). *Jurnal Studi Sosial Dan Politik*, *4*(1), 18–31. https://doi.org/10.19109/jssp.v4i1.5344

Pearlman, W., & Cunningham, K. G. (2012). Nonstate actors, fragmentation, and conflict processes. *Journal of Conflict Resolution*, *56*(1), 3–15. https://doi.org/10.1177/0022002711429669

Rahmadany, A. F., & Ahmad, M. (2021). The Implementation E-Government to Increase Democratic Participation: The Use of Mobile Government. *Jurnal Studi Sosi*, *5*(1), 22–34.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). 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*, *13*(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Rohali, S. M., & Yumitro, G. (2022). Women Terrorist Interests in the ISIS Movement: A Case Study in Indonesia. *Jurnal Studi Sosial Dan Politik*, *6*(1), 17–29. https://doi.org/https://doi.org/10.19109/jssp.v6i1.11141

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan*, *1*(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168. https://doi.org/10.30742/perspektif.v21i3.587

Sen, A. (2000). *Development As Freedom.*

Shafira, I. (2021). *Analyzing Indonesia's National Cybersecurity Strategy: Center for Digital Society.* Centre for Digital Society. https://cfds.fisipol.ugm.ac.id/id/2021/07/28/menganalisis-strategi-keamanan-siber-nasional-indonesia/

Sukarno, B., & Saleh, F. (2022). Vertical Conflict, Public Policies, and Pandemic Covid-19: Case Study of Central and Regional Government of DKI Jakarta. *Jurnal Studi Sosial Dan Politik*, *5*(1), 83–104. https://doi.org/https://doi.org/10.19109/jssp.v5i1.7904

Syed, S., & Ahmed, Z. (2021). Abraham Accords, Indo-Pacific Accord and the US-Led Nexus of Curtailment: Threat to Regional Security, and Joint Counter Strategy. *Policy Perspectives*, *18*(1), 25–52. https://doi.org/10.13169/polipers.18.1.0025

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law and Security Review*, *26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Westcott, N. (2008). The impact of the Internet on international Relations. *Oxford Internet Institute*, *July*. http://do.rulitru.ru/docs/22/21978/conv_1/file1.pdf

Wibowo, E. B., Legionosuko, T., & Mahroza, J. (2020). Industry 4.0: Challenges and opportunities in competency development for defense apparatus' human resources. *International Journal of Advanced Science and Technology*, *29*(7), 45–60.

Widarda, D. (2020). The Relationship Between Religion and the State for the Sovereignty of the NKRI Study of Suryalaya TQN Murshid Thought in the Tanbih Text. *Jurnal Studi Sosial Dan Politik*, *4*(2), 135–146. https://doi.org/10.19109/jssp.v4i2.6773

Yulianto, A. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *7*(1), 69–82. https://doi.org/10.21512/jas.v4i1.967

Zheng, T., Ardolino, M., Bacchetti, A., & Perona, M. (2021). The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review. *International Journal of Production Research*, *59*(6), 1922–1954. https://doi.org/10.1080/00207543.2020.1824085

Zotti, A. (2011). Inside cyber warfare. *Global Change, Peace & Security*, *23*(3), 437–438. https://doi.org/10.1080/14781158.2011.605638