Ilomata International Journal of Social Science
P-ISSN: 2714-898X; E-ISSN: 2714-8998
Volume 5, Issue 3, July 2024
Page No. 660-678

Implementation of Cyberspace Cooperation between Indonesia and United States A Combating Cyberterrorism in Indonesia, 2019–2023

Khoirunnisa[1], Minar Silvi[2], Evelin Angelina Rizqi Surya[3]
[12]Universitas 17 Agustus 1945 Jakarta, Indonesia
[3]Diakonisches Institut für Soziale Berufe, Germany
Correspondent: minarsilvi046@gmail.com[2]

Received : March 1, 2024
Accepted : July 2, 2024
Published : July 31, 2024

Citation: Khoirunnisa., Silvi, M., Surya, E, A, R. (2024). Implementation of Cyberspace Cooperation between Indonesia and United States A Combating Cyberterrorism in Indonesia, 2019–2023. Ilomata International Journal of Social Science, 5(3), 660-678.
https://doi.org/10.61194/ijss.v5i3.1173

ABSTRACT: This research focuses on the implementation of cyberspace cooperation between Indonesia and the United States in an effort to tackle cyber terrorism in Indonesia in the 2019-2023 period. The background of this research is based on the increasing cyber threats faced by Indonesia, including attacks on critical infrastructure and government data. This research uses a qualitative method with a literature study approach to collect and analyze data from various sources such as documents, books, journal articles, reports related to the problem to be solved, and publications related to cyber security and cyber diplomacy. The results show that cooperation between Indonesia and the United States has strengthened Indonesia's cyber defense capabilities through various initiatives, including incident management capacity building, national cyber strategy development, and information exchange. This cooperation is also supported by global cybersecurity policies and initiatives that involve both countries in international forums such as the ASEAN-US Cyber Policy Dialogue. This research concludes that cyberspace cooperation between Indonesia and the United States is a strategic step to address cyber threats and enhance security stability in the Southeast Asian region. Policy recommendations include further developing the cooperation framework and increasing cybersecurity awareness among the public.

Keywords: Implementation of Cyberspace Cooperation, Indonesia, United States, Cyberterrorism.

INTRODUCTION

The rapid development of information and communication technology in the digital era today has brought major changes in various areas of life, including security and terrorist threats. The threat of cyber attacks can be carried out systematically, effectively, efficiently and anonymously, disrupting, weakening or destroying the vital infrastructure functions of a country, and its impact and scope become very difficult to contain and predict. The combination of telecommunications, Internet, and broadcasting technologies has facilitated the emergence of broadband network infrastructure, which has also facilitated the emergence of new economies. On the one hand, this broadband network brings benefits to improve the quality of social and economic life, namely the

globalization of the digital economy (Chotimah, 2019; Glen, 2014). On the other hand, global broadband network connectivity is also a threat to all national assets. This global interconnection has created a cyber world characterized by online interaction, which offers many conveniences but also poses new vulnerabilities and threats, including threats to national cyber sovereignty.

However, the development of information and communication technology has made a positive contribution to the development of the world economy so that it has an impact on increasing productivity, competition, and community participation. However, as governments, businesses, and communities become more connected, the development of stronger cybersecurity requires greater attention to the challenges associated with cyber threats. According to ISO (International Organization for Standardization) ISO/IEC 27032, citing a number of sources, cybersecurity or cyber security is the maintenance of confidentiality, integrity, and availability of information in cyberspace. Cybersecurity refers to measures to protect information in cyberspace from various attacks (Budi, Wira, & Infantono, 2021; Cremer et al., 2022; Mueck, On, & Du Boispean, 2023; Norris, Mateczun, Joshi, & Finin, 2021).

Based on the results of the BSSN (State Cyber and Cryptography Agency) annual report "Cyber Security Monitoring Report 2018", the results of monitoring abnormal internet traffic nationwide from January to December 20182. It was revealed that there were 32,447,974 cases of internet traffic anomalies. Web network monitoring revealed 16,939 website incidents (defacement) due to cyberattacks on Indonesian networks, with go.id domains being the most frequently attacked domains. The threat of malware became the biggest threat for Indonesia in 2018, with 122 million activities recorded this year. In 2018, ID-SIRTII received a total of 2,885 incident reports from the public, four of which were complaints related to malware, fraud, DoS, and security vulnerabilities (*LAPORAN HASIL MONITORING KEAMANAN SIBER TAHUN 2018 - IDSIRTII*, n.d.).

International cooperation in countering cyber terrorism in Indonesia is carried out by establishing a cooperative relationship with the United States in the field of cyber security. The MoU, which encourages strong cooperation in the cyber sector, was signed in Jakarta on September 28, 2018 in Jakarta. The Government of Indonesia will be represented by Joseph R. Donovan, Jr., U.S. Ambassador to Indonesia, and H.E. Mohammad Anshor, Director of the Americas and Europe Bureau at the State Department. This MoU aims to build on existing partnerships and deepen cooperation in the cyber field that supports Indonesia's democracy and economic growth.

The Memorandum of Understanding that has been agreed will be a working framework to encourage and strengthen cooperation and facilitate the development of national cyber capabilities, including the State Cyber and Cryptography Agency (BSSN) which currently plays the role of the National Cyber Agency. BSSN is Indonesia's focal point which was formed to carry out tasks in the field of cybersecurity. The MoU focuses on several areas of cooperation, including the development of a national cyber strategy, national incident management capacity, capacity building and cooperation to combat cybercrime, discussions on cybersecurity awareness, and lastly, secondly, a national agreement to work on it. Consider an action plan to further identify the specific activities included in the MOU (U.S. Embassy Jakarta, 2018).

With the increasing number of forms of cybercrime in Indonesia, the main concern is whether the government can provide strong security in the cyber sector to overcome/deal with cybercrime. The form of cooperation between BSSN and BNPT to overcome the threat of terrorism in cyberspace is the focus of the Indonesian government in improving its security, in addition to critical infrastructure systems which are important national objects that are electronic-based and connected to the internet which can be a threat of terrorist attacks. As well as the involvement of cyberspace cooperation carried out by Indonesia and the United States in maintaining cyber security, the exchange of technology and knowledge, national interests, and legal policies in facing increasingly widespread cyber challenges.

In a previous study entitled "Implementation of Cyberspace Cooperation Between Indonesia and the United States in Increasing the Capacity to Handle Cyberterrorism Threats in Indonesia" written by Bimo Arya Putra. The results of the research discuss the concepts and theories of cyberpower, cyberpolitics, cyberterrorism, and security cooperation. The researcher focuses on cyber threats such as hacktivism, cyberspies, and cyberterrorism (Bimo Arya Putra, 2022). The difference between previous research and current research lies in the concepts and theories used. Previous research did not use concepts and theories such as cyber security and cyber diplomacy. And the research conducted by the previous study did not provide a research year that could be a reference for researchers in recommending strategic steps that must be taken by Indonesia regarding handling the threat of cyberterrorism. And this research was conducted to be able to reveal the effectiveness of cyber cooperation between Indonesia and the United States in combating cyber terrorism, which is a significant threat to Indonesia's national security.

Here are some questions that formulate the problem in the research: (1) What are the forms of cyberspace cooperation policies that have been carried out by Indonesia and the United States in dealing with the threat of cyberterrorism? (2) What are the challenges of cyberterrorism threats in Indonesia in 2019-2023?. (3) How is the implementation of cyberspace cooperation between Indonesia and the United States for Indonesia?

The purpose of this research is to analyze the implementation of cyberspace cooperation between Indonesia and the United States in an effort to eradicate cyber terrorism in Indonesia from 2019 to 2023. With a conceptual framework in the first section that examines the background of cyberspace cooperation between Indonesia and the United States and the formulation of the problem, the second section contains the theoretical basis for research such as; Cyber Security and Cyber Diplomacy theories, the third section examines related research methods, the next section contains results and discussions such as; cyberspace cooperation policies between Indonesia and the United States; analyzing the challenges of Cyberterrorism attack threats in Indonesia; and evaluating the implementation of this cooperation. The final section contains conclusions from the research analysis. It is hoped that this study can provide policy recommendations that can be adopted by both countries to strengthen cooperation in the field of cyber security and combat cyber terrorism.

Cybersecurity

Cybercrime has numerous variations, both at the person level and little bunches and organized wrongdoing bunches that assault and commit violations in an facilitated way. Cyber fear mongering could be an developing and genuine risk within the computerized age. Fear mongers have embraced the unused methodology of utilizing the Web as the essential implies of communication in their operations. They have moreover started utilizing counterfeit insights (AI) innovation to optimize cyber fear mongering assaults and exercises. In expansion, psychological militant bunches routinely utilize social media stages to spread their messages and belief systems and pick up modern adherents (Zaki, 2022).

The term terrorism can refer to an unlawful act of violence or crime against people to threaten a government, society, or group, sometimes to achieve political or other objectives. Terrorism is changing from its traditional structure to a form of terrorism supported by cyber innovations called cyberterrorism. Cyber terrorism is the use of cyberspace to deliver attacks to critical foundations that depend entirely on the existence of associations and states that can then drive their termination (Kalakuntla, Vanamala, & Kolipyaka, 2019).

Cyberterrorism can be carried out in a variety of ways, including distributed denial-of-service (DDoS) attacks, spreading malware, hacking systems, stealing data, and destroying information technology infrastructure. Cyberterrorism crimes can cause significant economic and non-economic losses to a country. So that terrorism crimes are a concern for every country to be able to overcome the level of cybercrime so that it is important to improve the cyber security system in a country.

Cybersecurity is a collection of tools, policies, security concepts, protections, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organizational and user assets. An organization's and users' cybersecurity assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and aggregated information transmitted and/or stored in the cyber environment. Cybersecurity is an effort to ensure the achievement and maintenance of the security characteristics of an organization and user resources from related security risks in the cyber environment (Ardiyanti, n.d.).

Cybersecurity is essential to protect and predict threats from cyberspace. Cybersecurity must be an ecosystem where laws, organizations, capabilities, collaboration, and technical implementation can run in harmony. There are many ways to improve or expand a country's cybersecurity, including improving domestic cyber capabilities and collaborating with other countries and international organizations (Primawanti & Pangestu, n.d.-a). And then in Indonesia is also promoting various policies and initiatives to build cybersecurity. One form of improving domestic cyber capabilities is the existence of the State Cyber and Cryptography Agency (BSSN), which is a government institution that is under and responsible to the president.

Cyber terrorism is a form of international crime that requires an overall improvement in cybersecurity to reduce the threat it poses. So that cyber security theory is an important foundation in efforts to overcome cyber terrorism crimes, because of the existence of forms of cybercrime

related to terrorism. By utilizing this theory, we can develop effective strategies and methods to deal with increasingly complex and dangerous cyber threats in the world of digital terrorism.

Cyber Diplomacy

The role of diplomacy is defined as an effort to gain support from individuals who significantly influence their views and actions. Therefore, each party involved in diplomacy is expected to be successful, harmonious, and emphasize the importance of quality relations. Diplomatic officials usually work together and coordinate, especially when dealing with complex issues. Effective problem-solving often requires maximum cooperation (Khoirunnisa & Jubaidi, 2024).

Cyber diplomacy can be translated as strategy in the internet, in other words the utilize of diplomatic resources and the usage of political functions to secure national interface related to the internet. These interface is ordinarily recognized in national the internet or cybersecurity methodologies and frequently incorporate references to political issues. Key issues on the cyber strategy plan incorporate cybersecurity, cybercrime, believe building, web opportunity, and web administration (Barrinha & Renard, 2017).

In the ever-evolving digital era, cybersecurity has become a top priority for countries around the world. International cooperation in cyberspace, especially between countries such as Indonesia and the United States, is very important. The theory of cyber diplomacy can help understand and develop a framework for cooperation to ensure both countries overcome challenges and take advantage of existing opportunities. In the theory of cyber diplomacy, there are several theories that are used as a reference in cooperation, such as the theory of collective security which states that cyber security cannot be achieved by one country alone and requires international cooperation. Cyber cooperation between Indonesia and the United States can be seen as an effort to build collective security in the Southeast Asian region and around the world. By sharing information on cyber threats and new technologies, both countries can strengthen their defenses against cyber attacks (Salsabilla Waskita & Sidik, 2023).

Cyber diplomacy is also driven by the national interest in protecting critical infrastructure and sensitive data from cyber threats. For Indonesia, cooperation with the United States will help strengthen the country's ability to deal with cyberattacks, which in turn will increase regional stability. This theory emphasizes the importance of cooperation to maintain stability in areas prone to cyber conflict. Cyber diplomacy involves developing legal and political frameworks that allow for effective cooperation. Indonesia and the United States need to coordinate their cyber policies to ensure cooperation occurs without legal barriers. This includes developing bilateral agreements and participating in multilateral initiatives to strengthen global cybersecurity.

Cyber diplomacy is also driven by national interests in protecting critical infrastructure and sensitive data from cyber threats. For Indonesia, cooperation with the United States will help strengthen the country's ability to deal with cyberattacks, which in turn will enhance regional stability. This theory emphasizes the importance of cooperation to maintain stability in areas prone to cyber conflict (Triwahyuni & Wulandari, n.d.). Cyber diplomacy involves developing legal and political frameworks that enable effective cooperation. Indonesia and the United States need to coordinate their cyber policies to ensure cooperation occurs without legal impediment. This

includes developing bilateral agreements and participating in multilateral initiatives to strengthen global cybersecurity.

METHOD

This research aims to describe and analyze the implementation of cyberspace cooperation between Indonesia and the United States in overcoming cyberterrorism in Indonesia in the 2019-2023 period. The main focus of the research is on the policies, challenges, and implementation of cyberspace cooperation between the two countries. This research uses a qualitative method with a literature study approach. This method involves collecting information and data from various sources such as documents, books, journal articles, and related reports. The literature study includes theoretical studies and scientific references relevant to the problem under study, as well as studying the results of previous similar research (Kurniawati, Seran, & Sigit, 2021). Qualitative research methods are based on the philosophy of postpositivism and are conducted in natural conditions. The researcher acts as a key instrument, with inductive data analysis and an emphasis on meaning rather than generalization(Sugiyono, 2019). This research uses cybersecurity and cyber diplomacy theories to analyze the concepts and strategies of cyberspace cooperation between Indonesia and the United States including policies, cyber capacity building, and the role of cyber diplomacy. In this research, the author discusses several cyberspace cooperation policies between Indonesia and the United States, such as the ASEAN-US Cyber Policy Dialogue, Cyber Intelligence and Information Exchange, and Cybersecurity Capacity Building Program. The analysis is conducted to identify the challenges and threats of cyberterrorism in Indonesia, understand the risks of various types of cyber attacks, and evaluate the implementation of the cooperation. The cyberspace cooperation between Indonesia and the United States is presented as a response to crimes that threaten national cyber security. This strategy is expected to improve the national cyber defense of both countries through policy, diplomacy, and cyber capacity building.

RESULT AND DISCUSSION

Cyber diplomacy between Indonesia and the United States was preceded by the growing cyber threats faced by both countries. Indonesia has experienced several cyberattacks targeting critical infrastructure and government data, highlighting the vulnerability of its digital systems. These threats come not only from state actors, but also from cybercrime groups and individuals with advanced technical skills. The United States is leveraging its experience and advanced technologies in cybersecurity to provide much-needed assistance to strengthen Indonesia's cyber defense capabilities. The goal of this Cooperation is to strengthen Indonesia's cyber infrastructure, improve data security, and protect critical infrastructure from evolving cyber threats (The White House, 2023).

In addition, this cooperation will also be influenced by global cybersecurity policies and initiatives. Both countries participate in various international forums on cybersecurity, including the ASEAN-US Cyber Policy Dialogue. Through this forum, Indonesia and the United States will work together

to address transnational cyber threats, share information on the latest threats and technologies, and develop joint policies and strategies to enhance regional and global cybersecurity. This cooperation reflects the commitment of both countries to contribute to international efforts to build a safe and stable digital environment. In addition, cyber diplomacy between Indonesia and the United States is also driven by the need to maintain regional stability in Southeast Asia, a strategic region vulnerable to cyber threats. Joint military exercises such as Super Garuda Shield are one of the two countries' concrete efforts to work together to strengthen preparedness and defense capabilities against cyber attacks (Joseph Rachman, 2023).

1. Cyberspace Cooperation Policy Between Indonesia and the United States

Cyber security approach in Indonesia in specific started in 2007 with the issuance of the Control of the Serve of Communication and Data Innovation Number 26/PER/M.Kominfo/5/2007 concerning Assurance of the Utilize of Web Protocol-Based Media transmission Systems. Besides, it was reexamined by Direction of the Serve of Communication and Data No.16/PER/M.KOMINFO/ October 2010, and after that upgraded with Direction of the Serve of Communication and Data No.29/PER/M.KOMINFO. /Dec 2010. One of the directions stipulated in this direction is the foundation of ID-SIRTII. ID-SIRTII stands for Indonesia Web Framework Security Occurrence Reaction Group, a group allotted by the Serve of Communication and Data Innovation (Kominfo) to assist screen Web security. Protocol-Based Media transmission Organize Back (Ramadhan, 2020).

The relationship between steadiness, security and smooth advancement got to be the premise for the foundation of the Affiliation of Southeast Asian Countries, or ASEAN for brief. As one of the pioneer nations of the foundation of ASEAN, Indonesia realizes that advancement at the national level must be based on secure and steady conditions at the territorial level. The Indonesian government has attempted different activities to secure the cyber world from the risk of cybercrime. One of the government's endeavors in keeping up data security in the internet is to utilize Law Number 36 of 1999 concerning broadcast communications and Law Number 36 of 2008 concerning Data and Exchanges as a premise in defining controls and arrangements related to data security receiving No. 11. In truth, the Indonesian government has too set up the State Cyber and Cryptography Agency (BSSN) which contains a mission to anticipate cyber assaults. BSSN moreover looks for to fortify the country's defense against cyber dangers and increment open mindfulness of cybersecurity (Putri, 2021).

ASEAN-US Cyber Policy Dialogue

ASEAN Territorial Gathering is one of the ASEAN gatherings that talks about worldwide issues. ARF is one of the sectoral organizations beneath the coordination of the ASEAN Chamber of the Political and Security Community. ARF members come from 26 nations and one European Union institution (a add up to of 27), as well as 10 ASEAN part states (Brunei, Cambodia, Indonesia, Laos, Myanmar, Malaysia, Philippines, Singapore, Thailand, and Vietnam) and 10 ASEAN nations have been built. Discourse accomplice nations (United States, Australia, Canada, China, India, Japan, Modern Zealand, Russia, South Korea, European Union) and seven other nations within the locale (Bangladesh, North Korea, Mongolia, Pakistan, Papua Modern Guinea, Sri Lanka, Timor-Leste). The term used to depict enrollment within the ARF is "Member." ARF is

additionally included within the areas of military, defense, customary exchanges on security issues are held.

The priority areas of cooperation discussed in the ARF consist of five main areas; (1) Disaster relief; (2) Eradication of terrorism and transnational crime; (3) Maritime Security; (4) Non-proliferation and disarmament; (5) Information and Communication Technology (Information and Communication Technology).

For each area of cooperation mentioned above, there is a work plan valid for two to three years, which contains the agenda, activities and content to be carried out during that period. Activities such as workshops, seminars, symposiums and training courses are also conducted to exchange information, deepen understanding and create networks that help build the capacity of government officials to deal with security issues (Primawanti & Pangestu, n.d.-b).

The composition of participants and the cooperation that occurs, it can be concluded that there are three possibilities; (1) For Indonesia, this forum is a forum to develop a culture of dialogue and cooperation to overcome differences and conflicts in the region. Indonesia also insists that the use or threat of violence is not an option to solve problems between countries; (2) Early warning system. Use this forum as an early warning system for the emergence of security issues that have not received or require attention from the Indonesian government; (3) Test the water. Let this forum be an opportunity to highlight important issues in Indonesia that have not received regional attention, to encourage other ARF participants to work together to address these issues.

The 4th ASEAN-U.S. Cyber Policy Dialogue will be held on October 19, 2023. The dialogue aims to create an open, peaceful, interoperable, reliable, and secure cyberspace that supports international trade and commerce, strengthens international security, and fosters economic prosperity, freedom of expression, and innovation. The United States and Indonesia are leading the dialogue. reminds us of the ASEAN-U.S. Summit Declaration on Cybersecurity Cooperation adopted at the 6th ASEAN-U.S. Summit in November 2018. The declaration reaffirmed the shared vision of a "peaceful, secure, and resilient regional cyberspace" and affirmed the holding of the ASEAN-U.S. meeting.

The Cyber Policy Dialogue will be held virtually on February 1, 2023. The dialogue facilitated the exchange of views on regional and international cyber environments, national cyber policies and priorities, including cooperation at international and regional levels. The dialogue reaffirmed its commitment to support and implement the Framework for Responsible State Conduct in Cyberspace, including ongoing discussions at the UN Public Working Group. The dialogue will highlight efforts to foster regional cybersecurity cooperation and capacity building, as well as the importance of implementing sustainable trust-building measures in cyberspace to reduce the risk of misunderstanding and escalation in cyberspace. This includes strengthening efforts at the ASEAN Ministerial Conference on Transnational Crime, the United Nations Convention to Combat Cybercrime, the ASEAN Ministerial Conference on Digital Issues, and the ASEAN Interregional Conference on Security and Use of Information and Communication Technology (BSSN, 2023).

Information Exchange and Cyber Intelligence

Participation between Indonesia and the United States within the field of data trade and cyber insights points to make strides the capacity of both nations to bargain with expanding cyber dangers. The organization incorporates an extent of activities and programs pointed at reinforcing cybersecurity framework, extending the workforce, and quickening reaction to cyber occurrences. The Cyber Data Sharing and Collaboration Program (CISCP) may be a program that empowers companies within the United States and its universal accomplices, counting Indonesia, to share data approximately cyber dangers in genuine time. The program is managed by the U.S. Office of Country Security's (DHS) Cybersecurity and Framework Security Organization (CISA).

The objective of the program is to move forward danger location and occurrence reaction through fast and successful trade of data between the open and private divisions. Locks in different government offices and private companies in Indonesia to share data and insights on the cyber dangers they confront (ISAO Standards Organization, 2015). As security dangers increment in the internet, checking potential dangers and assaults as a frame of defense in the internet gets to be exceptionally imperative. One strategy to perform this checking is through the utilize of honeypots. A honeypot is a pantomime framework for different administrations outlined to draw aggressors and track and consider their behavior, counting the strategies and procedures utilized.

Creating honeypots requires to be proceeded investigate into the number of administrations that must be imitated to keep pace with cyber advancements and the innovation utilized by assailants. No less critical is the collaboration of information trade between educate and organizations that have honeypots introduced in their framework. The collaboration aims to guarantee that the information obtained can be shared with other teach and organizations so that they can analyze the information together and foresee assaults some time recently they affect other organizations.

2019, there has been development and inquire about within the field of honeypot innovation. The center of this consider in 2019 was the Honeynet Risk Sharing Stage, which afterward advanced into the Collaborative Honeynet Danger Sharing Stage in 2020, and in 2021 got to be the Insights Honeynet Danger Sharing Stage. In 2022, previous developments have come about within the creation of a few open dashboards containing examination comes about data from different introduced honeypots. Another result is the availability of a committed entrance for each partner. Usually an institution or organization that has introduced a honeypot and permits partners to see information from the honeypot and download the information to utilize as investigate fabric for each partner (Honeynet, Layanan, & Bssn, 2023).

Cybersecurity Capacity Building Program

The cyber-security training and skills improvement program is carried out in coordination with the Cyber Defence Operation Centre Working Team. In addition, it is necessary to develop human resources about the importance of cyber-security in order to increase understanding of preventive measures in counteracting all acts of cybercrime. In order to develop human resource capacity in handling cyber-security, the TNI has collaborated with stakeholders who have capabilities in the field of Information Technology including cooperation carried out by the TNI AD with the Del Institute of Technology (IT Del), North Sumatra. This collaboration is planned to last for three

years, from 2014 to 2017 in three programs. The three programs include: preparation of cyber warfare models, seminars on military cyber intelligence and cyber operations, and cyber camps or cyber weeks (Ardiyanti, n.d.).

The establishment of CSIRT as one of the implementation of cyber security for cyber power development in Indonesia in accordance with Presidential Regulation Number 18 of 2020 concerning RPJMN 2020-2024 which mandates the establishment of 121 CSIRT as one of the strategic priority projects. The CSIRT team is tasked with minimizing and controlling damage due to cyber incidents by providing effective response and recovery, as well as preventing future cyber incidents. The presence of CSIRT will be the main force in order to oversee the information security system in MK. So that the presence of CSIRT is expected to be able to realize information security resilience in the Electronic-Based Government System (SPBE). BSSN in this case, of course, cannot stand alone, therefore it requires active participation of all parties in resolving incidents quickly, precisely and effectively. BSSN recommends that government institutions can immediately form CSIRT. With the increasing number of CSIRTs formed in the government sector, it is hoped that it will be able to build independence and readiness in facing the threat of cyber incidents and contribute directly to maintaining cyber security in Indonesia (Mahkamah Konstitusi Republik Indonesia, 2024).

2. Challenges of Cyberterrorism Threats in Indonesia in 2019-2023

Cybersecurity challenges and cyber strength in Indonesia can be partitioned into three fundamental columns: Control, Innovation, and Human Assets. In terms of law, there's still no law administering cybersecurity in Indonesia. The Cybersecurity and Cyber Flexibility Charge or the Cyber Security and Cyber Flexibility Charge was repudiated due to dissents over its arrangements that tie the commerce world. Subsequently, the issue is still subject to a few "comprehensive" controls with respect to the internet, such as the Law on Data and Electronic Exchanges (Law) Number 19 of 2016, Broadcast communications Law Number 36 of 1999, and Electronic Exchange Law Control No. 5. Controlled by directions. Service of Data and Communication on Web Protocol-Based Media transmission Arrange Security 2017 (Prabowo & Sihaloho, n.d.).

The scope of cyber psychological warfare must be constrained since the fast improvement of technology and data within the period of the Mechanical Insurgency 4.0 is. Some time recently continuing to this investigation, it is vital to get it the definition of cyberterrorism. Agreeing to the Center for Strategic and Universal Considers, cyber fear based oppression may be a arranged and politically spurred assault carried out by a gather, mystery specialist, or person against computer or data frameworks that seem physically affect non-combat targets Keith Rudo, delegate chief of the FBI's Cyber Division, said cyberterrorism may be a criminal act committed by a party possessing computer innovation or broadcast communications capabilities that causes savagery. Breakdown, or intrusion of administrations with the aim of inciting a fear reaction within the community makes it conceivable to happen. The point is to impact governments and social orders to recognize and bolster social, political and ideological challenges started by cyber fear based oppressors (Colarik, 2006).

Based on the study of I Putu Hadi Pradnyana and Muhammad Syaroni Rofii, examples of cyberterrorism incidents are divided into two categories: hybrid cyberterrorism and pure cyberterrorism. Hybrid cyber terrorism refers to cyberspace, specifically the Internet, which is used as a means of communication and coordination for the dissemination of propaganda, recruitment, financing, money laundering, and training of members. The Internet is used by terrorist groups to spread their ideological propaganda. The dissemination of various content such as photos and videos of assassinations, beheadings, executions, etc. carried out by terrorist organizations aims to cause fear among the general public, in addition to being a radicalization strategy. Pure cyber terrorism is a category that refers to direct attacks on the victim's cyber infrastructure, such as computers, networks, and the information stored on them. The fundamental goal is to achieve political, religious, and ideological goals (Pradnyana & Rofii, 2020).

The increment in cybercrime strengths the government to move forward its cybersecurity framework in arrange to bolster the progressively fast advanced change. One of the government's endeavors through the State Cyber and Cryptography Agency (BSSN) to bolster SPBE's cybersecurity in Indonesia is to oversee the introductory data of cyber assaults employing a honeynet framework. The BSSN honeynet framework is one of BSSN's open administrations that can be utilized by partners to supply data almost cyber assaults through honeypot gadgets executed by each partner. Data gotten from honeypot gadgets can be utilized by interested parties as input for border security devices and cybersecurity investigate materials.

Honeynet Global could be a non-profit organization dynamic within the field of information/cyber security around the world. Indonesia Honeynet Venture (IHP) could be a department built up in Indonesia. Indonesia Honeynet Venture (IHP) may be a department of the Indonesian Honeynet Extend (HN/P), a non-profit organization locked in in information/cybersecurity. IHP was propelled on November 25, 2011, based on a appeal of 15 individuals speaking to the scholarly community, intelligence/cybersecurity specialists, and government. This part proposed the foundation of Venture Honeynet – Indonesia department. This department is additionally bolstered ("Backed") by the Singapore department. IHP was formally built up on January 9, 2012, after getting endorsement from the Board of Chiefs of HN/P. The Honeynet Indonesia (IHP) extend centers on the discovery cycle of the cybersecurity system. Investigate conducted by IHP covering extortion procedures, discovery devices, information mining, malware discovery, cybercrime discovery, cryptography, and advance producing risk maps for utilize by the scholarly world, experts, government, and the business community will be actualized within the shape, and investigate will be conducted to encourage develop the risk sharing stage (*Laporan-Tahunan-Honeynet-Project-BSSN_IHP-2018*, n.d.).

Indonesia's cyber world was revitalized in 2019 through two major events. The first incident was related to a cyber incident that had a continuous impact on the national cybersecurity system, and the second incident was related to the government's efforts to strengthen national cybersecurity itself. For example, Garuda Mata BSSN is national surveillance system recorded 290.3 million cyberattacks in Indonesia in 2019. The biggest attacks came from American IP addresses, in contrast to last year when many registrations came from Indonesian IP addresses. alone. Malware cyberattack techniques are considered the most widespread in the global cyberworld. Hakumageddon found that 39 of the most common cyberattacks worldwide were malware attacks.

Malware attacks in Indonesia ranked first in the most commonly used attack techniques in 2019. 36.2% of the most common cyberattacks in Indonesia were recorded as malware attacks. In addition, Kaspersky records an average of 150,000 malware infections per month in Indonesia (Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2019).

In addition to malware, major cyber incidents such as data leaks and power outages have also occurred. Examples of data breaches include passenger data leaks at Lion Air's subsidiary, Malindo Air, and data leaks of 13 million Bukalapak accounts traded on dark sites. The nine-hour power outage on August 4, 2019 had a major impact on the internet network and digital businesses being run. As cyber threats become more sophisticated and on the rise in Indonesia, several other countries, including the United States, are also struggling to deal with the threat. According to the FBI, cybercrime in the United States resulted in losses of $ 3.5 billion or around Rp 47.9 trillion throughout 2019. Donna Gregory, director of the FBI's Internet Crime Complaint Center, said: "Criminals are becoming increasingly sophisticated, making it increasingly difficult for victims of fraud to tell which ones are real and which ones are fake. The second major development in Indonesia is the government's ongoing efforts to strengthen cyber defense (Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2019).

Based on data from the Honeynet Annual Report 2020, data on cyber attacks in Indonesia recorded 316,167,753 cyberattacks, of which 217,781 were recorded and one of the largest attacks was malware attacks. In 2021, there were 266,741,784 cyberattacks, 393,851 of which were malware attacks (*HONEYNET PROJECT BSSN-IHP L A P O R A N TA H U N A N*, 2021). Meanwhile, 370,022,283 cyberattacks were recorded in 2022, of which 812,192 were malware attacks, according to Honeynet's annual report data (REDAKSI Pelindung et al., 2023). Based on the 2023 Cyberattack Source Mapping conducted by verifying IP addresses, Indonesia is known to be the source country for the most cyber attacks. India ranks second with more than 147 million cases. There have been more than 89 million attacks in the United States and more than 34 million attacks in the United States. By 2023, the Honeynet system is expected to collect more than 600 million pieces of attack data. Of those cyberattacks, 1,093,503 were malware attacks. Various forms of cyberattacks are expected to occur in 2023. Among them are juicejacking attacks, phishing attacks through WhatsApp applications, banking, courier services, wedding invitations and online bookings, DarkPink APT attacks in ASEAN countries, ransomware attacks, and online gambling web destruction (Honeynet et al., 2023).

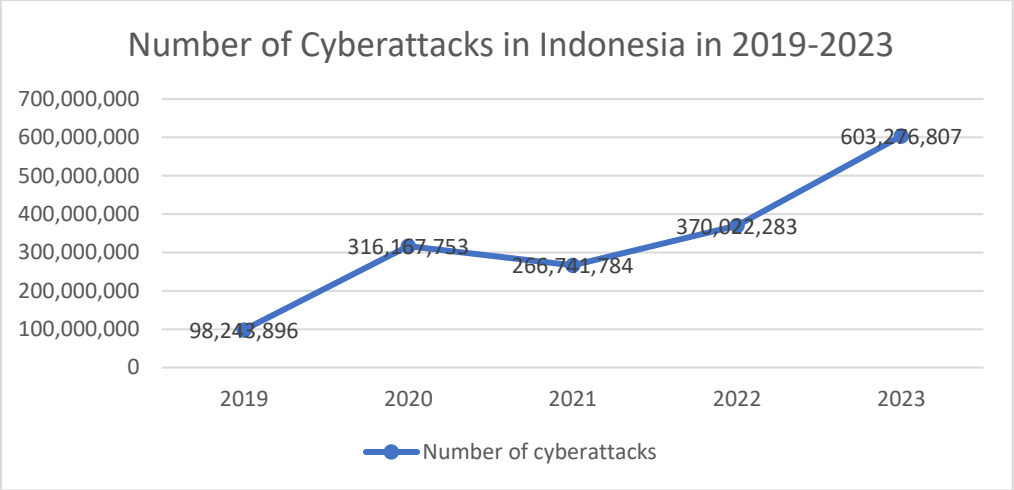

Figure 1. Graph of Cyberattacks in Indonesia

Source of: Annual Report of BSSN's Honeynet Project

3. Evaluation of the Implementation of Cyberspace Cooperation between Indonesia and the United States for Indonesia

Cyber participation between Indonesia and the United States may be a major center in two-sided relations, particularly given the developing cybersecurity challenges. The participation incorporates different key activities to fortify advanced foundation and improve the cybersecurity capabilities of both nations. As portion of the ASEAN-U.S. Cyber Arrangement Discourse, both nations are committed to working with other nations within the Southeast Asian locale to address territorial cyber dangers (United States Department of State, 2023).In expansion, President Joko Widodo's visit to the United States highlights key associations, counting specialized help and advanced capability upgrade (The White House, 2023).

The 4th ASEAN-U.S. Cyber Arrangement Dialogue will be held on October 19, 2023. The exchange points to make an open, tranquil, interoperable, dependable, and secure the internet that underpins worldwide exchange and commerce, fortifies worldwide security, and cultivates financial thriving, flexibility of expression, and development. The United States and Indonesia are driving the exchange. Reminds us of the ASEAN-U.S. Summit Statement on Cybersecurity Participation received at the 6th ASEAN-U.S. Summit in November 2018. The announcement reaffirmed the shared vision of a "quiet, secure, and strong territorial the internet" and confirmed the holding of the ASEAN-U.S. assembly.

The Cyber Approach Discourse will be held for all intents and purposes on February 1, 2023. The discourse encouraged the exchange of views on territorial and worldwide cyber situations, national cyber approaches and needs, counting participation at worldwide and territorial levels. The exchange reaffirmed its commitment to bolster and execute the System for Dependable State Conduct in The internet, counting continuous talks at the UN Open Working Bunch. The exchange will highlight endeavors to cultivate territorial cybersecurity participation and capacity

building, as well as the significance of executing maintainable trust-building measures in the internet to decrease the hazard of misconception and heightening in the internet.

This incorporates reinforcing endeavors at the ASEAN Ecclesiastical Conference on Transnational Wrongdoing, the Joined together Countries Tradition to Combat Cybercrime, the ASEAN Ecclesiastical Conference on Advanced Issues, and the ASEAN Interregional Conference on Security and Utilize of Data and Communication Innovation. The discourse too promised to fortify capacity-building endeavors and territorial participation within the field of cybersecurity. The discourse incorporates, among others, reinforcing territorial participation in cyber capacity building through cybersecurity activities and programs, such as the U.S.-Singapore Third Nation Cybersecurity Preparing Program, Computerized Network and Cybersecurity Organization, and ASEAN-Japan, ASEAN-Singapore Capacity Building and Cybersecurity Discourse Center, Center of Brilliance - ASEAN's endeavors to fortify its capacity to secure basic framework, counting mechanical control frameworks, and battling cybercrime. The discourse cultivates participation between the U.S and ASEAN as sketched out within the ASEAN-U.S. Vital Activity Arrange, the ASEAN-U.S. Comprehensive Vital Organization, and the ASEAN Viewpoint Standards and Vision for the Indo-Pacific and ASEAN 2025 Network Ace Arrange (Novitasari, n.d.).

Through BSSN as well, the government points to arrange endeavors and assets to preserve security in the internet, counting ensuring basic framework and basic government information. Mindfulness and participation are key to building solid guards against fear based oppressor dangers, counting in the computerized domain. In this setting, interagency participation is fundamental to combat the danger of cyber fear based oppression. BSSN works closely with different government offices and covers viewpoints of cybersecurity, extending from policing, counter-terrorism and money related examination to universal relations and defense (Hendra Wicaksana et al., n.d.).

Through coordination with these various sectors, the Indonesian government points to battle the danger of cybercrime comprehensively and successfully. The association of different services and organizations in cybersecurity endeavors appears how genuine the Indonesian government is in tending to the complex challenges postured by the advanced world. This expanded collaboration between divisions is anticipated to empower a speedy and productive reaction to expanding cyber dangers (Khoirunnisa & Jubaidi, 2024).

Within The Joined together States, cybersecurity operations are classified as DHS (Division of Wellbeing and Human Administrations) country security operations. Division of Defense (DoD) and Government Bureau of Examination (FBI). DHS is mindful for internal security. DHS incorporates a National Cyber Security Division whose mission is to work with open, private, and international organizations to ensure the internet and U.S. interface in the internet. The division encompasses a National Cyber Reaction Coordination Bunch, which comprises of 13 government organizations and is mindful for planning the government government's reaction to cyber incidents affecting the nation (Rosy, 2020).

To combat dangers, cyberattacks, and high-tech wrongdoing, the FBI built up the FBI's Cyber Division to supervise national endeavors to explore and indict cybercrimes, counting cyber fear based oppression, surveillance, computer interruption, and acts of cyber extortion. the internet.

The mission is carried out by the National Joint Cyber Examination Errand Constrain (NCIJTF). NCIJTF is commanded by the President of the U.S to serve as the essential point of contact for all government offices to arrange, coordinated, and coordinated all information related to cyber risk investigations (Setiyawan, 2019).

Indonesia is collaborating with the U.S within the field of cybersecurity since of the pressing have to be move forward national cyber defense capabilities in the confront of progressively complex dangers. An illustration of the significance of this participation is the hacking of the Indonesian government's data framework that happened a few a long time back. The assault highlights vulnerabilities in Indonesia's digital infrastructure and highlights the ought to progress cybersecurity through more progressed innovation and ability. Through this association, Indonesia will have got to to the most recent cybersecurity innovations and best hones created by the Joined together States. For case, through the ASEAN-U.S. Cyber Arrangement Discourse, Indonesia can take an interest in territorial endeavors to upgrade cybersecurity and secure basic information from worldwide dangers (United States Department of State, 2023).

In expansion, joint military works out such as the "Super Garuda Shield" will offer assistance Indonesia create a more viable cyber defense procedure, fortify operational capabilities, and fortify participation between nations in countering cyber assaults (Joseph Rachman, 2023). Subsequently, participation with the United States will not as it were offer assistance Indonesia combat cyber dangers, but moreover fortify its position on the territorial and worldwide cybersecurity outline.

CONCLUSION

Several important conclusions can be drawn based on the results of cyber diplomacy discussions between Indonesia and the United States. First, increasingly large and complex cyber threats force Indonesia to strengthen its security infrastructure. Attacks on critical infrastructure and Indonesian government data have highlighted the vulnerability of the country's digital systems. The United States, with its technological excellence and cybersecurity expertise, has become a strategic partner to help Indonesia meet these challenges. This cooperation aims to strengthen Indonesia's cyber infrastructure, improve data security, and protect critical infrastructure from growing threats.

Second, this cooperation is also supported by the participation of the two countries in international forums such as the ASEAN-US Cyber Policy Dialogue. At this forum, Indonesia and the United States will work together to address cross-border cyber threats, share information on the latest threats and technologies, and develop joint policies and strategies to improve regional and global cybersecurity. In addition, cyber diplomacy also aims to maintain stability in Southeast Asia, a strategically important region that is vulnerable to cyber threats. Joint military exercises such as Super Garuda Shield are a clear example of the two countries' efforts to strengthen preparedness and defense capabilities against cyber attacks.

Finally, the cybersecurity policy and various legislative initiatives implemented by Indonesia, such as the establishment of ID-SIRTII and BSSN, demonstrate the government's commitment to improving cyber resilience. Meanwhile, the Cyber Intelligence and Information Sharing Program

with the United States under the Cyber Information Sharing and Collaboration Program (CISCP) strengthens threat detection and incident response through rapid and effective information exchange. All of these efforts reflect the importance of international cooperation to address increasingly complex and diverse cyber threats. Overall, the study shows that cyber diplomacy between Indonesia and the United States is a strategic step to enhance cybersecurity, protect critical infrastructure, and strengthen regional cooperation to address rising cyber threats.

REFERENCE

Ardiyanti, H. (n.d.). *CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA*. Retrieved from http://kominfo.go.id/index.php/content/detail/3980/

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

Bimo Arya Putra. (2022). *Implementasi Kerjasama Ruang Siber Antara Indonesia dan Amerika Serikat Dalam Meningkatkan Kapasitas Penanganan Ancaman Cyberterrorism di Indonesia*. Universitas Pembangunan Nasional Veteran Jakarta.

BSSN. (2023, November 8). BSSN Bertindak Sebagai Co-Chair Indonesia Pada Kegiatan The 4th ASEAN-US Cyber Policy Dialogue. *Bssn.Go.Ig*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

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. *Riwayat Artikel Diterima*, *10*(2). https://doi.org/10.22212/jp.v10i1.1447

Colarik, A. (2006). *Cyber terrorism: political and economic implications*. Idea Group Inc (IGI).

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics and Policy*, *42*(5), 635–657. https://doi.org/10.1111/polp.12093

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (n.d.). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. https://doi.org/10.33164/iptekkom.22.2.2020.143-158

Honeynet, L., Layanan, B., & Bssn, H. (2023). *B E R K O L A B O R A S I D E N G A N I H P.*

HONEYNET PROJECT BSSN-IHP L A P O R A N TA H U N A N. (2021).

ISAO Standards Organization. (2015). Cyber Information Sharing and Collaboration Program (CISCP). *Isao.Org*.

Joseph Rachman. (2023, September 14). US-Indonesia Security Relations Flourish in a Changing Indo-Pacific. *Thediplomat.Com* .

Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber Security. *HOLISTICA – Journal of Business and Public Administration*, *10*(2), 115–128. https://doi.org/10.2478/hjbpa-2019-0020

Khoirunnisa, K. ;, Jubaidi, D., & Khoirunnisa, K. (2024). 49-Journal of Diplomacy and International Relations (PJDIR) published by the International Relations Study Program, Faculty of Social and Political Sciences, Cenderawasih University, in collaboration with the Indonesian Association for International Relations (AIHII). *Papua Journal of Diplomacy and International Relations*, *4*(1), 49–66. https://doi.org/10.31957/pjdir.v4i1.3447

Khoirunnisa[1], K., & Jubaidi[2], D. (2024). *Politeia : Journal of Public Administration and Political Science and International Relations Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism*. https://doi.org/10.61978/politeia.v2i1

Kurniawati, A., Seran, A., & Sigit, R. R. (2021). *Teori Kritis dan Dialektika Pencerahan Max Horkheimer*. *10*(2), 124. Retrieved from www.publikasi.unitri.ac.id

LAPORAN HASIL MONITORING KEAMANAN SIBER TAHUN 2018 - IDSIRTII. (n.d.).

Laporan-Tahunan-Honeynet-Project-BSSN_IHP-2018. (n.d.).

Mahkamah Konstitusi Republik Indonesia. (2024). Pentingnya Pembentukan CSIRT untuk Antisipasi Insiden Siber. *Mahkamah Konstitusi Republik Indonesia*.

Mueck, M. D., On, A. E. B., & Du Boispean, S. (2023). Upcoming European Regulations on Artificial Intelligence and Cybersecurity. *IEEE Communications Magazine*, *61*(7), 98–102. https://doi.org/10.1109/MCOM.004.2200612

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173–1195. https://doi.org/10.1080/07352166.2020.1727295

Novitasari, I. (n.d.). BABAK BARU REJIM KEAMANAN SIBER DI ASIA TENGGARA MENYOSONG ASEAN CONNECTIVITY 2025. In *Cyber Security Cooperation in South East Asia* (Vol. 1). ASEAN Connectivity. Retrieved from ASEAN Connectivity website: http://ejournal.uki.ac.id/index.php/japs/article/view/624

Prabowo, T. B., & Sihaloho, R. A. (n.d.). *ANALISIS KETERGANTUNGAN INDONESIA PADA TEKNOLOGI ASING DALAM SEKTOR ENERGI DAN DAMPAKNYA PADA KEAMANAN NASIONAL ANALYSIS OF INDONESIA DEPENDENCE ON FOREIGN TECHNOLOGY IN THE ENERGY SECTOR AND ITS IMPACT ON NATIONAL SECURITY*.

Pradnyana, I. P. H., & Rofii, M. S. (2020). Ancaman Cyberterrorism di Indonesia dan Respons Negara. *LITERATUS*, *2*(2), 181–191. https://doi.org/10.37010/lit.v2i2.92

Primawanti, H., & Pangestu, S. (n.d.-a). *DIPLOMASI SIBER INDONESIA DALAM MENINGKATKAN KEAMANAN SIBER MELALUI ASSOCIATION OF SOUTH EAST ASIAN NATION (ASEAN) REGIONAL FORUM*.

Primawanti, H., & Pangestu, S. (n.d.-b). *DIPLOMASI SIBER INDONESIA DALAM MENINGKATKAN KEAMANAN SIBER MELALUI ASSOCIATION OF SOUTH EAST ASIAN NATION (ASEAN) REGIONAL FORUM*.

Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara. (2019). *Laporan Tahunan 2019 Pusopskamsinas*.

Putri, K. (2021). Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime. *Jurnal Hukum Lex Generalis*, *2*(7).

Ramadhan, I. (2020). STRATEGI KEAMANAN CYBER SECURITY DI KAWASAN ASIA TENGGARA. *Jurnal Asia Pacific Studies*, *3*(2), 181–192. https://doi.org/10.33541/japs.v3i1.1081

REDAKSI Pelindung, T., Badan Siber dan Sandi Negara Pengarah, K., Jenderal TNI Dominggus Pakel, M., Penanggung Jawab, M., Yusuf, A., Pemimpin Redaksi, M., … Jimmy, St. (2023). *LAPORAN TAHUNAN 2022 HONEYNET PROJECT BSSN IHP*.

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

Salsabilla Waskita, A., & Sidik, H. (2023). Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. *Padjadjaran Journal of International Relations*, *5*(2), 142–164. https://doi.org/10.24198/padjirv5i2.41337

Setiyawan, A. (2019). NATIONAL CYBERSECURITY POLICY IN THE U.S AND INDONESIA. *UNTAG Law Review (ULREV)*, *3*(1), 71–87. Retrieved from http://inet.detik.com/read/2012/01/20/105656/1820779/323/7-negara-asean-yang-paling-sering-kena-

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D / Sugiyono* (Ed. 2 ; Cet. 1). Bandung : Alfabeta, 2019.

The White House. (2023, November 13). *FACT SHEET: President Joseph R. Biden and President Joko Widodo Announce the U.S.-Indonesia Comprehensive Strategic Partnership*.

Triwahyuni, D., & Wulandari, T. A. (n.d.). *STRATEGI KEAMANAN CYBER AMERIKA SERIKAT*. Retrieved from http://www.census.gov/population/www/popc

United States Department of State. (2023, November 7). *Co-Chairs' Statement on the Fourth ASEAN-U.S. Cyber Policy Dialogue*.

U.S. Embassy Jakarta. (2018, October). Indonesia dan Amerika Serikat Sepakat Memajukan Kerja Sama Ruang Siber. *Kedutaan Besar Dan Konsulat AS Di Indonesia* .

Zaki, M. M. (2022). Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime. *Jurist-Diction*, *5*(3), 973–988. https://doi.org/10.20473/jd.v5i3.35790