Available online at: http://journal.uinsgd.ac.id/index.php/ks
Khazanah Sosial, Vol. 5 No. 2: 359-367

DOI: 10.15575/ks.v5i2.26414

Counter Cyber Terrorism Governance In Indonesia

Arlan Siddha[1*], Renaldo Benarrivo[1]

[1]Universitas Jenderal Achmad Yani, Cimahi, Indonesia
*Corresponding Author E-mail: arlan.siddha@lecture.unjani.ac.id

Abstract

In the contemporary landscape, the rapid evolution of information and communication technology (ICT) exerts a profound and multifaceted impact, shaping diverse aspects of daily life while concurrently introducing complex dynamics into the political-security domain, particularly in Indonesia. The consequences of ICT utilization hinge on its intent, and the absence of effective regulation transforms it into a dual-edged instrument. Within this context, the spectrum of threats has expanded and transformed, encompassing traditional religion-based terrorism and the emerging frontier of cyber-based terrorism. This paper offers a balanced examination of Indonesia's response to cyber terrorism, employing qualitative research methods to interpret existing data and formulate a governance framework for countering this evolving threat. Indonesia has judiciously identified domestic conditions for resource optimization while actively pursuing international cooperation to enhance its capabilities. Nevertheless, persistent challenges persist in the governance of cyber terrorism countermeasures, notably institutional barriers and organizational culture, posing obstacles to effective coordination among relevant institutions in Indonesia.

Keywords: Governance, counter-terrorism, cyber terrorism, international cooperation, cyber security.

Abstrak

Dalam konteks masa kini, pesatnya evolusi teknologi informasi dan komunikasi (TIK) memberikan dampak yang mendalam dan beragam, membentuk beragam aspek kehidupan sehari-hari sekaligus membawa dinamika kompleks ke dalam ranah politik-keamanan, khususnya di Indonesia. Konsekuensi pemanfaatan TIK bergantung pada tujuannya, dan tidak adanya regulasi yang efektif menjadikannya instrumen bermata dua. Dalam konteks ini, spektrum ancaman telah meluas dan bertransformasi, mencakup terorisme berbasis agama tradisional dan terorisme berbasis dunia maya yang sedang berkembang. Makalah ini menawarkan kajian yang seimbang mengenai respons Indonesia terhadap terorisme dunia maya, dengan menggunakan metode penelitian kualitatif untuk menafsirkan data yang ada dan merumuskan kerangka tata kelola untuk melawan ancaman yang terus berkembang ini. Indonesia telah secara bijaksana mengidentifikasi kondisi dalam negeri untuk optimalisasi sumber daya sambil secara aktif mengupayakan kerja sama internasional untuk meningkatkan kemampuannya. Namun demikian, masih terdapat tantangan dalam tata kelola penanggulangan terorisme siber, terutama hambatan kelembagaan dan budaya organisasi, sehingga menghambat koordinasi yang efektif antar lembaga terkait di Indonesia.

Kata kunci: Pemerintahan, kontra-terorisme, terorisme siber, kerja sama internasional, keamanan siber.

INTRODUCTION

The existence of the internet as part of the development of information and communication technology is an important milestone that marks various kinds of multidimensional novelties in the 21st

Received: Juny 12, 2023; Revised: August 1, 2023; Accepted: August 14, 2023

century. In 2021 internet users worldwide reached 63% (World Bank, 2020). The significance of using the internet provides various opportunities as well as challenges that need to be addressed wisely, not only at the level of individual internet users but also at the state level. This is important to note considering that if left without proper governance, the use of the internet can lead to crisis conditions, both in the political-security, economic and socio-cultural contexts. Related to terrorism issues for instance, the impact of cyber terrorism cannot be considered trivial, this is because the world is increasingly interconnected, both in terms of information and communication.

The phenomena of crime that use cyber as a medium of crime also continues to develop along with the development of technology itself. Starting from the theft of important data, whether in the form of personal data directed at manipulating credit card transactions, for example, to data in the form of important state information. Therefore, this is absolutely important to serve as a common concern, and the role of the state is needed to be present, and organize the internet and all its developments so that the internet can then be optimized for the benefit of the community and the state. Instead, it becomes a new form of threat that can have a negative impact. The United Nations Office on Drugs and Crime (UNODC) explains that this is a cross-border crime that develops in cyberspace by actors spread across various regions and has a global impact (United Nations Office on Drug and Crime, 2019).

Novelty in this article lies in the examination of Indonesia's response to the evolving threat of cyber terrorism, which is becoming increasingly complex and interconnected in our digital age. The article takes a comprehensive approach, considering both domestic conditions and international cooperation in countering cyber terrorism. It sheds light on the delicate balance needed in governing the use of information and communication technology to prevent it from becoming a double-edged sword. Moreover, it highlights the importance of addressing institutional barriers and organizational culture as key factors influencing the coordination between various entities involved in countering cyber terrorism within Indonesia. This holistic perspective on governance and security in the digital realm provides valuable insights into the challenges and opportunities faced by Indonesia in tackling this pressing issue.

RESEARCH METHOD

The research method used in searching for research-related data is using qualitative methods. Qualitative method is one of the methods used in researching a phenomenon in socio-political studies. Generally, qualitative methods are methods used in scientific research that are descriptive. Data in qualitative research are not in the form of numbers, but words, sentences, and systematic narratives, which describe an event, symptom, and phenomenon with the analysis of certain theories and concepts (Subagyo, 2020).

The scope of location for this research is Indonesia. This is because Indonesia is also a country that cannot be separated from the threat of cyber terrorism. The governance of terrorism in Indonesia also still requires many continuous adjustments in order to be able to eliminate the potential threat of cyber terrorism. The time limit for this research is 2017. This refers to the cyber terrorism case of the Ransomware WannaCry virus in 2017 which affected Indonesia from cyber attacks.

The data collection technique used in this research is to use written sources such as library research and structured interviews. Written sources in the form of books, dissertations, scientific journals, and curriculum vitae are valuable written sources for research as a source of library data (Anggito & Setiawan, 2018). While the interview is a question-and-answer activity to obtain information or data (Lubis, 2018).

According to Bogdan and Biklen in providing an understanding that qualitative research methodology is a research procedure that produces descriptive data in the form of writing or statements.

 ISSN 2715-8071 (online)

Analyzing previous sources that already exist in research. It refers to the phenomenon that will be discussed regarding human behavior in interacting with other people. In using natural data analysis techniques that are descriptive, do not use numerical calculations in analyzing data inductively (Bogdan & Biklen, 1997).

RESULTS AND DISCUSSION

The Growing Threats of Cyber-Terrorism

Crimes committed anonymously (without a name) make cybercrime a crime that is difficult to detect. Referring to the 5th UNODC Conference in 2010 that cybercrime is one of the organized transnational crimes and is considered one of the emerging crimes (Maskun et al., 2013). The complexity, whether in the context of actors, issues or patterns of relationships, or interactions that occur in them, makes the state must make maximum efforts to pay attention to the dynamics in its strategic environment. National, regional and global dynamics must be considered in determining what steps the state will take to tackle cyber terrorism. The issue of crime is increasingly emerging, especially when it comes to the platform used. Transnational crime is developing so rapidly with various modus operandi, including terrorism which also makes digital space to carry out its actions in spreading fear.

This is what drives Indonesia to conduct security cooperation, especially in dealing with cyber security issues in the type of cyber terrorism crime (cyber terrorism). So a security cooperation framework was formed, one of which discussed the recognition of global threats such as international terrorism that could threaten military or non-military security. This framework of cooperation must of course also reflect the governance of counter-terrorism at the national level so that then there are no gray areas that become potential problems in the governance of countering cyber-terrorism in Indonesia. Although the issue of terrorism has existed dominantly during the cold war and after, the climax of the strengthening of this phenomenon was the outbreak of the tragedy of the WTC and the US Pentagon, on September 11, 2001 (Subagyo, 2015). The 9/11 tragedy seemed to be a new milestone in the discourse on terrorism globally. Public awareness is awakened to the importance of counter-terrorism efforts that can be carried out through international cooperation schemes.

According to James H. Wolfe's terminology in Waliyanri & Syauqillah (2022), the targets of acts of terrorism can be civilian targets (supermarkets, schools, places of worship, hospitals, and other public facilities) as well as non-civil targets (military facilities/camps). The presence of the internet as a new hybrid of technology allows acts of terrorism to be carried out through computers. The term cyber terrorism was first proposed by Barry C. Collin in the 1980s (N. K. Kadir et al., 2019). Collin claims that cyber terrorism is a convergence of encounters between the physical world and the virtual world that meet as a result of an act of cyber terrorism (U.S Department Of Justice, 2020). Space and time have lost their relevance in the context of cyber terrorism, so the state needs to rethink what kind of response is appropriate in the form of policies related to governance in tackling cyber terrorism. This study aims to analyze and propose strategies for counter-cyber terrorism governance in Indonesia especially with an outward looking action that reflecting inward-looking policies.

In 2017 the world was shocked by the spread of a computer virus called the WannaCry Ransomware which paralyzed more than 200,000 computers in more than 150 countries (GOV-CSIRT INDONESIA, 2019). A criminal group called Shadow Brokers who are members of the Lazarus Group terrorism group are known to be responsible for the spread of the virus as an act of cyber terrorism. This phenomenon has an impact on Indonesia, which attacks hospital computer operations, including Harapan

Kita Hospital and Dharmais Hospital Jakarta (A. Kadir, 2017). The security threats that have occurred have become more apparent over time, even the WannaCry Ransomware attacks are still occurring today, so that banks labeled state-owned enterprises cannot be separated from becoming victims. Seeing the phenomenon of cyber threats that are increasingly affecting state security, this study takes the title "Counter Cyber Terrorism Governance in Indonesia."

Cyber Security

The development of the digital transformation era in the 21st century has had a great influence and impact on human life. One of the negative impacts of digital-based crime is called cyber crime. This of course refers to the security of the cybercrime that gave rise to cyber security. Cyber security is an effort to protect information network systems in network devices that contain important data belonging to individuals, the private sector, and the government. Another definition states that cyber security is a collection of policy tools, security concepts, assurance management, and technologies to protect the cyber environment and user assets. Just as security, in general, does not yet have a definite definition, there is also no clear definition of cyber security to explain a cyber phenomenon. The lack of clarity in this definition is also compounded by the exponential development of information and communication technology, so that the reactions carried out will always be too late for the development of the phenomenon itself.

Cyber security is present as an effort to prevent and at the same time handle the problem of cybercrime in the form of cyber attacks that can attack anytime and anywhere. This global threat in the 21st century has penetrated cyber crime where previously there were four urgent issues for global threats such as terrorism, refugee crisis, natural disasters, and global warming (Patel & Chudasama, 2021). Typology of threats to cyber security can vary, Myriam Dunn in the journal Asia Pacific Studies explains these threats into three typologies: cyber crime, cyber war, and cyber terrorism. Cybercrime is a criminal activity that uses information technology to achieve the economic interests carried out by criminal organizations. While Cyberwar is a form of a digital version of Von Clausewitz's war and Cyber terrorism is an activity of hacking or disabling the information system of the nation-state carried out by terrorist groups (Ramadhan, 2019). From a series of existing terrorism phenomena, especially in the context of using cyber as a medium to manifest its actions, cyber terrorism has now become a new form of security that needs to be responded to appropriately.

Cyber security was chosen as a concept from the basis for the preparation of cyber terrorism counter measures governance. This can be seen from the urgency of cyber activities that produce negative impacts such as cybercrime. The influence of globalization and the rapid development of information technology has made cybercrimes penetrate the world of terror called cyber terrorism. After the 9/11 incident at the WTC New York Building, acts of terrorism have become a serious threat to countries in the world. The conservative approach can no longer be used, its relevance has been eroded by the development of information and communication technology itself. Cyberterrorism is not a phenomenon that can be solved only by relying on militaristic efforts, or even strengthening aspects of law enforcement alone.

Cyber Terrorism

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives (Plotnek &

Slay, 2019). The enemy they face is no longer an attacker with a tank filled with explosives or a vest filled with dynamite on a person's body, but attacks with the tap of a button on electronic media such as computers or mobile phones. In carrying out their actions, terrorist groups use cyberspace to cause damage. Terrorists fight against the government for certain purposes and they will use various means to achieve these goals (Rachmat, 2015). The concept of cyber terrorism needs to be interpreted strategically by the Indonesian government to be able to formulate its policy framework.

The Threat of Cyber Terrorism in Indonesia

The development of terrorism in Indonesia experiences changes in patterns and motives at every event. Terror acts in Indonesia can be distinguished based on three forms, namely, revolutionary movements aimed at changing the political economy of the current regime (such as the Indonesian Communist Party), ethno-nationalist terrorists are separatist movements that have the goal of establishing their state and separate from the sovereignty of the Republic of Indonesia. such as the Free Aceh Movement (GAM) and the Free Papua Organization (OPM) and religious terrorism who use religion as a guide for their actions (Darul Islam and Jemaah Islamiyah) (Univeritas Kristen Indonesia, 2019). The change of government from the old order to the reformation also influenced every act and motive of terror. If in general, the old order attacked places of worship out of distaste for other religious minorities, in the reform era the attacks were aimed at the public directly, such as bombing restaurants, hotels, or even shopping centers.

The increasingly complex acts of terrorism in Indonesia have penetrated the cyber world, namely cyber terrorism. As a country that has a high number of internet users, Indonesia is often a target for acts of terror. This is due to the weakness of the system and applications. Distributed Denial of Service (DNS) attacks on systems with .id or .co.id domains become website domains that are often hacked by hackers to spread their acts of terror. An independent and sovereign country certainly wants the development of digital-based state facilities, including Indonesia. Computer-based public facilities such as banking systems or e-commerce have a risk of terrorism crimes. The types of cyber terrorism crimes that often occur in Indonesia are ATM card or personal account burglary and electronic transactions (m-banking).

In addition, Indonesia has also formed several governments and non-government agencies or institutions to prevent acts of cyber terrorism. These agencies include the National Cyber and Crypto Agency (BSSN) which is under the direct leadership of the President, the Ministry of Defense established the Cyber Defense Center (Pushansiber), and Kominfo which has formed a team known as the Indonesia Security Incident Response Team on Internet Infrastructure. /Coordination Center (Id-SIRTII/CC). The thing that should be considered is to establish coordination and communication between institutions so that there is no misunderstanding or misperception among cyber security institutions for the national interest of Indonesia. Periodic development of digital systems and updating of existing technology can be done as an initial step to prevent new cyber threats.

BSSN states that the cyber terrorism act in Indonesia is still at level three. This level is categorized as the lowest level, which means that the target users are still individuals or the general public. Cyberattacks at the social strata use more social media platforms such as spreading propaganda, radicalism, and recruiting members on public websites (Firmansyah, 2020). However, this level three attack is considered the most dangerous because it directly attacks users without passing through a massive security system. Social media has become a target for spreading at level three for terrorists to carry out their actions. This is related to the security system of each individual's social media user and some countries do not regulate their society in the use of social media platforms, including Indonesia.

Another case is that Indonesia was once one of the countries affected by cyber terrorism attacks in the form of a virus (malware) called Stuxnet (Kompas.com, 2010). One of function of the Stuxnet virus is used to spy on the system being sabotaged. Kaspersky Lab from the US said that Stuxnet is a prototype cyber weapon that will lead to the creation of a new competitive power in the world. Then in 2017, the world was shocked again by the case of the spread of a computer virus called Ransomware Wannacry which was allegedly masterminded by a cyber-terrorist group. And Indonesia is again affected by the spread of the computer virus.

BSSN as Indonesia's Cyber Security Gate

BSSN was present at the fusion of three previous institutions, namely the National Crypto Agency, the Directorate General of Applications and Information Technology and the Ministry of Communication and Information. Since the establishment of BSSN, all matters related to the world of digitalization have become the responsibility of the independent institution. BSSN is also a digital certification authority as stated in PP No. 82 of 2012 concerning the Use of Electronic Systems and Transactions (Pratama, 2018). The WannaCry ransomware case that attacked the world including Indonesia in 2017 made cyber terrorism cases a new "task" for BSSN that must be considered and make a quick win work target. Learning from the success of the market in forming habits in society through information system architecture, the information system architecture approach should be adopted by BSSN to regulate cyberspace (Pratama, 2017).

From an outward-looking perspective, it can be seen from BSSN's view that not all areas of cooperation in countering cyber terrorism are running as expected. International cooperation carried out by Indonesia in dealing with cyber terrorism is generally within the scope of Risk and Governance. Risk and Governance are the scopes that regulate laws and protect data. So that if some ongoing attacks and threats attack the computer systems of the community/agencies, it is not the task of the national cyber security agency, but has returned to the decision of each individual. While the situation of the WannaCry ransomware attack that occurred is within the scope of maintenance. It is left to each company or institution whose computer is infected to have an IT expert. However, some opinions say that there is still a lack of BSSN as a National Cyber Institute for Indonesia. First, there is a misunderstanding between the concepts of information security (information security) and cyber security (cyber security). The scope of cyber security is wider than just "maintaining" information security but rather securing digital and non-digital records such as secret service notes, company documents, printouts of proof of payment (ATM), and cyber assets themselves (Azmi, 2018). So that the regulator and the coordination of the technical functions of the BSSN have a double assignment.

First, the BSSN is formed as a regulator maker, and the second serves as a technical officer instead of engaging in cyber security directly (Azmi, 2018). The WannaCry Ransomware which attacked almost 200,000 computers in the world at that time made BSSN a regulator maker and its technical functions collide. The ransomware, which was allegedly launched by Advanced Persistent Threat (APT) by North Korea's Lazarus Group, was allegedly the mastermind behind the WannaCry attack. APT is an attack through a network campaign where the intruder builds a highly sensitive data system in the long run. APT actors are usually affiliated with the government which is the state actor in cyber-terrorism cases. So it is impossible for state-class attacks that are masterminded by state actors to be handled by one institution that has a dual role and task in presenting cyber security.

 ISSN 2715-8071 (online)

Directions for Managing Cyber Terrorism in Indonesia

Improving Cyber Security HR in Indonesia

Human Resources in the technological era is no less important in the role of dealing with the increasingly sophisticated cyber world. Computer operating systems still require humans as manual operators of the computer system itself. But in reality, there are still many shortages of human resources who understand the progress of science and technology or IT experts around the world. Human resources who have expertise in dealing with cyber threats are a real need. Of course, in practice, human resources need to be managed well, so that their capabilities are maintained and continually improved. In its internal efforts, Indonesia through The Ministry of Communication and Information and in collaboration with PT. Xynexis created a cyber security talent search program called Born to Control in 2017 which recruits a minimum of 2000 talents in the cyber security sphere to solve cyber security system problems. However, only 100 people will be selected from 1000 prospective registrants who take part in Digicamp born to protect or the so-called gladiators of the Indonesian cyber world. The Ministry of Communication and Information stated that it is grateful to have a BSSN institution that specifically regulates cyber threats in Indonesia (Kemenkominfo, 2018). Realizing that this digitalized world has entered the Internet of Things (IoT) aspect, Indonesia is also trying to carry out its external cooperation through international security cooperation with strategic partner countries.

The cyber boot camp program that was carried out in 2018, for example, has had a significant impact, especially on Indonesia. This is evident from the 2018 GCI report that Indonesia is in 4th place in the Southeast Asian region and 41st position globally. The head of BSSN said that the results now obtained are based on Indonesia's hard work to establish cooperation with any parties and agencies for the benefit of both parties (Detik.Com, 2019). In the two years since the establishment of the BSSN in 2017 Indonesia incised a fairly rapid cyber development until 2019. This is inseparable from various actors or related parties (stakeholders) in success in guarding Indonesian cybersecurity for the better. For services from the internal sector, the BSSN Electrical Certification Center has issued as many as 62,183 electronic certificates used in 187 agencies consisting of 37 central governments and SOEs as well as 150 local governments (BUMD) and universities in Indonesia (Kure, 2019). This indicates an increase in competence and connections in increasing the number of cyber experts and staff at BSSN.

Literacy Enrichment on Cybersecurity

Indonesia's vision and mission in campaigning for internet users that are open, free, and safe in the scope of cyber security seem to have been seen. The practice of international cooperation carried out by Indonesia is cooperative and influences and encourages Indonesia to continue to make innovative programs. One of them is to create a seminar program for the general public about safe internet education through the Cyber Security Literacy Campaign by BSSN or known as Kli KS. This campaign was successfully held in several big cities in Indonesia such as Yogyakarta, Surabaya, and Jakarta. These seminars and educational activities for the community provide awareness of personal data security to form a positive culture with the need for technology and secure information (BSSN, 2018).

More than 500 participants attended this seminar with various backgrounds and have the same intention, namely increasing cybersecurity awareness and practical knowledge that they can implement. The spread of fake news (hoaxes) and suspicious information on social media such as spreading propaganda or understanding radicalism became the speaker's theme on this year's KliKs occasion. In addition, the impact resulting from the Cyber Boot Camp under the Third Cyber Policy Dialogue agenda

provides easy access for the Indonesian people to access information related to cyber security on the BSSN website more easily accessible. The services available include, namely, PID (Information and Documentation Management Officer) which provides services for requesting public information, Honeynet (a system for detecting cyber threats based on malicious software), Electronic Certificates, APROKSI (Information Security Protection Assistance), GOV-CSIRT, HR Consultation, and Information Technology Security Assessment (ITZA). This certainly provides space and convenience for the people of Indonesia in finding sources of information related to cyber security that is safe and reliable.

CONCLUSION

In 2017 active internet users worldwide have reached 51%, which indicates that half of the world's population can access the internet network easily. Industry 4.0 makes it easier to surf in cyberspace (cyberspace) more freely but brings the other side, namely the negative impacts such as cybercrime resulting from the facilities available. Transnational crimes such as acts of terrorism can now be carried out using electronic media because they are the result of the convergence of original crimes with technological sophistication (cyber terrorism). The management of cyber-terrorism will bring certainty to the legal basis governing the course of countering cyber terrorism in Indonesia. The arrangement will also provide a strong justification to encourage bilateral dialogue, exchange of personnel and/or information, and the implementation of activities that are expected to be cooperative. The WannarCry Ransomware attack in 2017 which attacked almost 150 countries and 200,000 computers in the world, including Indonesia, made security cooperation in the cyber sphere more concerned. Cyber security for a country in the 21st century carries an urgency that is as important as the security of its maritime, air and land territorial areas. The collaboration between Indonesia through BSSN and its counterparts provides a dynamic space for cybersecurity. Indonesia realizes that the increased potential for cyber development will result in stronger threats, so a binding cyber collaboration is needed. The direction that needs to be generated from the implementation of cyber terrorism management is the increase in cyber security human resources in Indonesia, the formation of the development of ideas and research, and the implementation of literacy campaigns on cyber security.

REFERENCES

Anggito, A., & Setiawan, J. (2018). *Metodologi penelitian kualitatif*. CV Jejak (Jejak Publisher).

Azmi, R. (2018). *BSSN Dua Kuasa Dalam Satu Tubuh Mengapa Bermasalah?* https://theconversation.com/badan-siber-dan-sandi-negara-dua-kuasa-dalam-satu-tubuh-mengapa-bermasalah-94224

Bogdan, R., & Biklen, S. K. (1997). *Qualitative research for education*. Allyn & Bacon Boston, MA.

BSSN. (2018). *Kampanye Literasi Keamanan Siber BSSN Sukses Digelar di Yogyakarta*. BSSN. https://bssn.go.id/kampanye-literasi-keamanan-siber-bssn-sukses-digelar-di-yogyakarta

Detik.Com. (2019). *BSSN: Keamanan Siber Indonesia Naik Peringkat*. Detik.Com. https://inet.detik.com/security/d-4774115/bssn-keamanan-siber-indonesia-naik-peringkat

Firmansyah, M. (2020). *Aksi Terorisme Ranah Siber di Indonesia Masih di Level 3*. Alinea.Id. https://www.alinea.id/nasional/bssn-ragukan-kesiapan-transformasi-digital

GOV-CSIRT INDONESIA. (2019). *Hati-hati! Serangan Ransomware Wannacry Belum Berkahir", internet. retrieved time 22.05 PM.* Govcsirt.Bssn.Go.Id. https://govcsirt.bssn.go.id/hati-hati-serangan-ransomware-wannacry-belum-berakhir/

Kadir, A. (2017). *RS Dharmais Terinfeksi Virus Wannacry*. CNN Business. https://www.youtube.com/watch?v=WgjKRP39j5A

Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes. *Fiat Justisia: Jurnal Ilmu Hukum*, *13*(4), 333–344.

Kemenkominfo. (2018). *Born to Protect Siapkan Gladiator Dunia Siber Indonesia*. Kemenkominfo. https://kominfo.go.id/content/detail/14903/born-to-protect-siapkan-gladiator-dunia-siber indonesia/0/berita_satker

Kompas.com. (2010). *Stuxnet Bentuk Terorisme di Dunia Maya*. Kompas.Com. https://ekonomi.kompas.com/read/2010/10/04/23054037/stuxnet.bentuk.terorisme.di.dunia.maya

Kure, E. (2019). *BSSN Beberkan 2 Tahun Kawal Keamanan Siber*. Investor.Id. https://investor.id/it-and-telecommunication/200548/bssn-beberkan-2-tahun-kawal-keamanan-siber

Lubis, M. S. (2018). *Metodologi penelitian*. Deepublish.

Maskun, M., Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. *Masalah-Masalah Hukum*, *42*(4), 511–519.

Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. *National Journal of Cyber Security Law*, *4*(1), 12-20p.

Plotnek, J. J., & Slay, J. (2019). What is cyber terrorism: Discussion of definition and taxonomy. *Conference Proceedings of 18th Australian Cyber Warfare Conference 2019*, 1–4.

Pratama, B. (2017). *Menaruh Harapan Pada Badan Siber Nasional*. Business Law.Binus.Ac.Id.

Pratama, B. (2018). *Badan Siber dan Sandi Negara Tantangan Membangun Kedaulatan Siber*. Binus Univeristy Faculty of Humanities. https://businesslaw.binus.ac.id/2018/01/30/badan-siber-dan-sandi-negara-dan-tantangan-membangun-kedaulatan-siber/

Rachmat, A. N. (2015). *Keamanan Global: Transformasi Isu Keamanan Pasca Perang Dingin*. Penerbit Alfabeta.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*, *3*(2), 181–192.

Subagyo, A. (2015). *Teroris (Me): Aktor & Isu Global Abad XXI*. Alfabeta.

Subagyo, A. (2020). *Aplikasi Metode Riset: Praktik Penelitian Kualitatif, Kuantitatif, dan Mix Methods*. Inteligensia Media.

U.S Department Of Justice. (2020). *Future of Cyberterrorism: The Physical and Virtual Worlds Converge*. Www.Ojp.Gov. https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual worlds-converge

United Nations Office on Drug and Crime. (2019). *Cybercrime*. UNODC. https://www.unodc.org/unodc/en/cybercrime/index.html

Univeritas Kristen Indonesia. (2019). *Buku Perkembangan Terorisme di Indonesia*. Univeritas Kristen Indonesia. http://repository.uki.ac.id/432/1/Buku Perkembangan Terorism20di Indonesi.pdf

Waliyanri, A., & Syauqillah, M. (2022). Lone Wolf Terrorism Trends in Indonesia. *International Journal of Science and Society*, *4*(3), 372–384.

World Bank. (2020). *Individuals Using Internet (% of Population)*. World Bank. https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&start=2021&view=bar