Continuous Inter-Country Cooperation in Facing Cyber Threats and Indonesia's National Security Challenges

Mifdal Zusron Alfaqi, Abd. Mu'id Aris Shofa, Muhammad Mujtaba Habibi, Rika Safitri Nur Azizah

[1] Department of Law and Citizenship, Faculty of Social Sciences, State University of Malang
mifdal.zusron.fis@um.ac.id

Abstract. Cooperation between countries in dealing with cyber threats and challenges to national security in the digital era is becoming increasingly important. This study uses the literature review method to answer three objectives. First, to describe the forms of cooperation between countries that can be carried out in dealing with cyber threats and challenges to national security in the digital era. Second, to explain the factors that can influence the success of cooperation between countries in dealing with cyber threats and challenges to national security in the digital era. Third, to describe the impact of sustainable cooperation between countries in dealing with cyber threats and national security challenges in the digital era on global security and international stability. The findings of this study show that cooperation between countries in terms of developing regulations, increasing capacity, and exchanging information can be effective in dealing with cyber threats and challenges to national security in the digital era. Factors such as trust, openness, and active involvement of all parties can influence the success of cooperation between countries. The impact of continued cooperation between countries in dealing with cyber threats and challenges to national security in the digital era includes increasing global security and international stability.

Keywords: Indonesian Security, between countries, Cyber Crime.

1 Introduction

The world that is increasingly connected globally through the internet and other information technologies carries a great risk of potential and cyber threats to a country including Indonesia (Chotimah, 2019). This context indicates the ability of the internet to eliminate geographical boundaries makes cyber attacks that are carried out from anywhere more fertile and more difficult to identify and control by one country such as cyberespionage, and electronic fraud that can harm the interests of the country. According to Ahyati, et all (2021) the digital era has a significant impact on human life throughout the world, especially in terms of communication, trade, and national defense.

The advantages provided by digital technology also open up opportunities for cybercriminals and conflicting countries to exploit it for their own benefit.Sulistianingsih (2022). According to Rizaldi (2022) cyber attacks can resemble malware, ransomware,

E. Yafie et al. (eds.), *Proceedings of the 5th International Conference on Humanities and Social Science (ICHSS 2024)*, Advances in Social Science, Education and Humanities Research 901,
https://doi.org/10.2991/978-2-38476-352-8_14

and DDoS (Distributed Denial of Service) attacks that are increasingly difficult to overcome by one country alone, and require strong cooperation between countries. The more information and transactions are carried out online, the more vulnerable data and system security is. Countries need to work together in terms of developing the implementation of cyber security policies and sharing information on the threats they face and helping each other investigate and prosecute criminals who carry out attacks from their respective territories (Nainggolan, 2019). This problem requires international cooperation in the field of cyber security which is carried out in a sustainable and continuous manner in order to provide optimal and effective protection for the country and its citizens.

A country's defense against cyber attacks requires the involvement of various aspects, including policies, strategies, technology, and human resources. The country must have clear policies and regulations to regulate the use of information technology including data privacy policies. Strict regulations will force compliance with high security standards through a mature security strategy that includes tactics and technologies used to detect, prevent, and respond to cyber attacks (Yudistriansyah, 2019). These problems require investment in cyber defense including various things such as the development of security technology and strengthening of technological infrastructure. Some examples of massive investments in cyber defense are made by the United States, which spent more than $ 18 billion in fiscal year 2022 on cyber security and information defense (Hajiansyah, et al; 2022).

Even the European Union plans to spend more than €2.5 billion to improve cybersecurity across Europe in the period 2021-2027. Countries and organizations are also increasing international cooperation in this area to improve global cyber capabilities and security. In this context, a balanced approach is still needed between the development of security technology and human rights. Cybersecurity policies that are too strict can endanger a person's privacy and freedom, so the development of security technology must be balanced with adequate and transparent privacy policies, as in Indonesia.

The above problems require a solution to digital crimes that threaten domestic security through several objectives of writing this article, namely: 1) describing the form of cooperation between countries that can be done to deal with cyber threats and national security challenges in the digital era; 2) explaining the factors that can influence the success of cooperation between countries in dealing with cyber threats and national security challenges in the digital era; 3) describing the impact of ongoing cooperation between countries in dealing with cyber threats and national security challenges in the digital era on global security and international stability. The method used is a qualitative literature review method that collects and analyzes articles, books, and documents related to international cooperation in dealing with national security challenges in the digital era selected from the Google Scholar, ScienceDirect, and ACM Digital Library databases.

The expected benefits of the results of this study are a) theoretically it can be a reference for further researchers who will conduct research on cyber cooperation carried out by Indonesia as part of national defense; b) practically for the government it can help to find a cyber handling strategy that is in accordance with its characteristics so as to be able to reduce the significant impact permanently on cyber actions. On the other

hand, for the community it can be used as study material in assessing the government's success in handling cyber.

2 Literature Review

2.1 Cyber in Indonesia

In Indonesia, handling of Indonesian cyber is through the establishment of a special institution to handle cybercrime, namely the National Cyber and Crypto Agency (BSSN) which is responsible for national cybersecurity and collaborates with related institutions, both domestically and abroad. However, these efforts do not guarantee a reduction in the risk of cybercrime in Indonesia. Cyber threats can endanger a country's national security through attacks on infrastructure such as electricity systems, transportation systems, and telecommunications systems, which can disrupt the stability of the country (Babys, 2021). Even according to Harianja (2022) cyber attacks can cause the cessation of economic activities in a country which causes instability and social conflict in society. Other fields such as politics are also easy targets for hoax information, political propaganda that can influence election results and the political stability of a country. Therefore, every country must have an effective cybersecurity strategy and policy to protect the country from cyber threats. The country must also have a team that is trained and able to respond quickly to cyber attacks (Triwahyuni, 2017). In addition, public awareness of cybersecurity is also very important to minimize the risk of cyber attacks. If a country is unable to protect its information technology infrastructure from cyber attacks, significant impacts will be felt in the economic, defense, and political sectors. To protect the country's cyber security, the government must adopt effective strategies and policies in identifying, preventing, and responding to cyber attacks through international cooperation in the field of cyber security is also very important to overcome cross-border cyber attacks.

2.2 Threats and National Security Challenges in the Digital Era

Cooperation between countries in dealing with cyber threats and national security challenges in the digital era can be done in several ways, including: 1) Exchange of information related to cyber threats they face in the form of intelligence data, information about new technologies, or ways to deal with cyber attacks. Countries can share information about malware or viruses that are spreading, hacking techniques used, and strategies to overcome these attacks through international organizations such as INTERPOL and Europol can play an important role as mediators between countries; 2) Tracking and arresting cyber criminals by strengthening cooperation between law enforcement and cyber security agencies in various countries; 3) Establishment of uniform rules and regulations related to cyber security, thus facilitating coordination and cooperation between different countries in dealing with cyber threats; 4) Establishment of a special team consisting of cyber security experts and representatives from related institutions to monitor and deal with emerging cyber threats. Countries can form a joint team consisting of cyber security experts to study attacks that occur and develop strategies to

overcome these attacks. This joint team can consist of cyber security experts from several countries to improve the quality and quantity of information obtained; 5) Conducting joint training to improve the capabilities of cybersecurity experts in dealing with cyber attacks through training and new techniques in cybersecurity, such as machine learning, artificial intelligence, and working together to develop cybersecurity standards that can be adopted by all countries as standards and strategies to address cyberattacks (Riski, 2022).

3 Methodology

The research method used in this study is a narrative review as a type of research that collects different research results and compares them to produce a holistic interpretation. A comprehensive overview of the topic of cyber security and cooperation carried out by Indonesia allows researchers to review and consider all available literature by comparing and synthesizing the results of various different studies. According to Yusuf (2019) the literature review method is a process of collecting, analyzing, and synthesizing information from literature sources that are relevant to a particular research topic with the aim of gaining a better understanding of the selected research topic, as well as identifying knowledge gaps that can be filled by subsequent research.

The literature review method allows researchers to identify areas where further research is needed and where gaps in research occur that can provide valuable information without having to conduct empirical research (Cahyono, 2019). To conduct a narrative review, researchers must explicitly determine literature search criteria and inclusion criteria. The stages of narrative review research consist of three stages, the first is determining the focus of the research, urgency, novelty, formulation, and objectives of the research (Rukin, 2019). The second is conducting a literature search with keywords that are relevant to the research topic. The third is writing the results of the analysis and looking for new points that can be analysis findings (Gasparyan, 2011).

The literature search in this study was conducted on various databases such as Sciencedirect, Google Scholar, WoS, and Garuda. The keywords used are cooperation in handling Cyber, Cyber in Indonesia, Cyber security challenges in Indonesia. The inclusion criteria set for conducting literature selection are that articles are written scientifically and are relevant to the research topic, articles can be accessed in full, and articles are prioritized as the latest. After that, combine information points sourced from various literatures into a whole unit and are presented in more depth for future research or to answer practical needs. These information points are then presented in more depth for future research or to answer practical needs. After that, the next step is to find new evidence-based points that can be analysis findings.

4 Result and Discussion

4.1 Forms of Cooperation Between Countries That Indonesia Can Undertake to Face Cyber Threats and National Security Challenges in the Digital Era

Indonesia has carried out various collaborations in dealing with cybercrime, including: 1) ASEAN Ministerial Meeting on Transnational Crime (AMMTC) Cybercrime Working Group to combat cybercrime in the ASEAN region through coordination between member countries. In this collaboration, Indonesia contributes to the preparation of regulations and development of national and regional capacities in dealing with cybercrime. 2) Cooperation with the FBI and Interpol in the exchange of intelligence information, training, and technical assistance in investigating cybercrime involving perpetrators from several countries. 3) Cooperation with technology and information security companies to improve protection against cybercrime attacks including the provision of security equipment and consulting services in dealing with cybercrime. 4) Cyber Defense Center as a cybersecurity control center that aims to prevent and handle cybercrime attacks that occur in Indonesia. This center collaborates with government agencies and the private sector in developing the latest strategies and technologies to address cybercrime attacks (Nugraha, 2021).

Cooperation between countries in terms of cybersecurity is not only useful for protecting digital infrastructure, but also for protecting society from increasingly rampant cybercrime. Countries must work together to develop effective and efficient cybersecurity policies and practices, and strengthen cooperation in the fields of intelligence and law enforcement (Sudarmadi, 2019). National security challenges in the digital era cannot be overcome by one country alone, but require close cooperation between the countries involved. In this case, ongoing cooperation between countries will enable the exchange of information and technology, as well as assistance in dealing with cyber attacks and other national security threats. This brings other benefits, including increased international trade and investment, exchange of technology and expertise, and the development of stronger diplomatic relations between countries. In this increasingly complex digital era, cooperation between countries is key to creating a safe and stable cyberspace for everyone (Babys, 2021).

Forms of cooperation between countries that Indonesia can do to face cyber threats and national security challenges in the digital era are: 1) conducting more intense bilateral cooperation with countries that have sufficient capabilities and experience in the field of cyber security such as the United States (having organizations such as the NSA, FBI, and CIA that specialize in cyber security and intelligence) and England with the GCHQ (Government Communications Headquarters) agency. In this cooperation, Indonesia can share information and experience in dealing with cyber threats and conduct training and development of security technology together; 2) Conducting multilateral cooperation by joining international organizations to face cyber threats and national security challenges together. Through this cooperation, Indonesia can participate in the formation of international cyber security standards and strengthen diplomatic relations with other countries; 4) Strengthening Cyber Defense Partnership through cyber defense partnerships with other countries to face cyber threats and strengthen national

security defense. In this partnership, Indonesia can share intelligence information and cyber security technology and conduct joint exercises in dealing with possible cyber threat scenarios (Rahmawati, 2020).

4.2 Factors That Can Influence the Success of Cooperation Between Countries in Facing Cyber Threats and National Security Challenges in the Digital Era

Cooperation between countries in dealing with cybercrime is very important and crucial in efforts to combat criminal acts involving information and communication technology. Because the nature of cybercrime does not recognize national borders, cooperation between countries is very necessary to strengthen and accelerate law enforcement efforts in cyberspace (Herdanto, 2022). Success factors are needed to handle cybercrime because cybercrime is increasing and increasingly complex, and can have a negative impact on individuals, companies, and even the country as a whole. In handling cybercrime, success factors are very important to measure the effectiveness of cybersecurity programs and strategies implemented by individuals, companies, and governments. Without clear success factors, it is difficult to know whether the efforts made have been effective in protecting sensitive data and information from cyber attacks. Success factors can include a number of things, such as: 1) Increasing cybersecurity awareness and skills among the general public, company employees, and government personnel; 2) Building a strong cybersecurity system that can identify and respond to cyber attacks quickly and effectively; 3) Developing strict regulations to prevent cybercrime and provide strict sanctions for perpetrators of cybercrime; 4) Provide continuous training and education for cybersecurity personnel to deal with increasingly complex and evolving threats; 5) Establish cooperation and collaboration with other stakeholders, such as companies and other countries, in dealing with cross-border cyber threats (Khoironi, 2020). By considering these success factors, handling cybercrime can be more effective and can reduce the negative impact of cyber attacks.

Cooperation between countries in dealing with cyber threats and national security challenges in the digital era can be influenced by several factors, including: 1) Clear and similar policies and regulations in dealing with cyber threats and national security challenges. This can help reduce differences in perception and strengthen cooperation between countries; 2) A high level of trust is needed and building strong and trusting relationships with each other; 3) Countries must have adequate skills and expertise in dealing with cyber threats and national security challenges. This includes capabilities in information technology, cybersecurity, and intelligence; 4) Openness of information can help countries understand the threats they face and strengthen cooperation between countries in dealing with these threats. Countries must share information about the cyber threats and attacks they face openly. 5) The role of the private sector; 6) adequate capacity and resources to deal with cyber threats and national security challenges including sufficient budget, trained personnel, and sophisticated technology; 7) Sustainability to strengthen their capacity and improve their skills and expertise in dealing with these threats (Irawati, 2021)

Competence and skills in mastering defense technology have a very high importance. However, these skills cannot be obtained easily. Human investment processes such as training or technology transfer are needed to develop these skills. The superiority of a country's defense depends on the ability to utilize the potential of existing human resources, not only through increasing quantity, but also quality such as special skills, physical and moral skills (Anwar, 2018). In addition, technical knowledge must also be expanded in defense equipment. Therefore, the role of education is very important because human resources are one of the main factors in development and defense. Individuals who have high human capital will have a positive impact on national defense and also the economy, because they can become qualified workers. From now on, the defense structure must be changed to suit the increasingly unconventional form of war in the future. The form of war will increasingly involve modern military technology, which is owned by the country's human resources. Attacks are not only carried out by state actors, but also by guerrillas and non-state militias who attack countries quickly, such as the attack on the World Trade Center (WTC) in the United States. In the future, human resources will no longer be the only dominant element in battle, but weapons technology will also be very important to win the battle. Special skills, such as advanced IT skills such as hacking and cyber warfare, will be very important to deal with asymmetric warfare. Threats will also come in the form of electronic warfare, information warfare, cyber warfare, and psychological warfare. Therefore, there needs to be an adjustment in the defense structure to deal with increasingly complex and unpredictable forms of warfare in the future.

4.3 The Impact of Sustainable Cooperation Between Countries in Facing Cyber Threats and National Security Challenges in the Digital Era on Global Security and International Stability

Sustainable cooperation between countries is essential in dealing with cyber threats and national security challenges in the digital era. Cyber threats can affect global security and international stability, given the increasing dependence on digital technology and the internet in our daily lives. Some of the positive impacts of cooperation between countries in this regard include: 1) Increasing effectiveness in dealing with cyber threats: with cooperation between countries, better coordination can be created in dealing with cyber threats. Countries can share information and experiences about tactics and strategies that have been successfully used in dealing with the same threats. 2) Reducing the risk of conflict between countries: Cooperation between countries in the field of cyber security can help strengthen diplomatic relations and reduce the risk of conflict between countries. Countries can find agreement and solve common problems in a peaceful manner. 3) Encouraging technological development: Cooperation between countries in the field of cyber security can also encourage the development of safer and more reliable technology. Countries can share knowledge about the latest technology, develop stricter security standards, and promote innovation in cyber security (Yanuarti, 2020).

Some challenges in cooperation between countries in dealing with cyber threats and national security challenges in the digital era. These challenges include: 1) Differences

in security policies so that it is sometimes difficult to reach the same agreement in dealing with cyber threats. This can complicate cooperation efforts between countries; 2) Technological limitations where countries that are more technologically advanced may find it difficult to share their technology and knowledge with less advanced countries. 3) National security issues are the reason some countries are reluctant to share information about their national security with other countries because they are worried that it could endanger their national interests (Nastiti, 2017). In facing these challenges, it is important for countries to keep communication channels open and strengthen cooperation in dealing with cyber threats and national security challenges in the digital era. Countries also need to increase understanding and awareness of the importance of cyber security and develop effective strategies to deal with it.

There are several factors that can complicate cooperation in handling cyber between countries according to Nenden (2020), including: 1) Differences in Law and Policy where each country has different rules and policies related to handling cybercrime. These differences in law and policy can cause problems of incompatibility between one country and another. For example, actions that are considered illegal in one country may not be considered illegal in another country. This can complicate the process of extraditing cybercriminals; 2) Differences in culture and language where each country has a different culture and language. These differences can cause difficulties in understanding information obtained from other countries, especially if the information is translated from the original language into another language; 3) Each country has national security interests that must be maintained. Countries may not be willing to share information about their national security with other countries, even if the information can help in handling cybercrime; 4) Countries with more advanced technology may find it more difficult to cooperate with countries with less advanced technology. This can lead to differences in the ability to handle cybercrime, and also affect how information and technology can be shared between countries; 5) Political competition between countries can lead to distrust and suspicion between countries. This can make it difficult to cooperate in handling cybercrime; 6) Limited budget and available resources can make it difficult for countries to handle cybercrime. Countries may not be able to provide the necessary resources to assist other countries in handling cybercrime.

5 Conclusion

Countrymust cooperate with other countries and international organizations to strengthen cyber defense involving the exchange of information and cooperation in developing advanced security technologies and countering mutually beneficial cyber threats. First, the form of cooperation between countries that can be carried out to face cyber threats and national security challenges in the digital era includes: 1) Exchange of information and intelligence on existing cyber threats and how to overcome these threats; 2) Cooperation in the development of technology and security standards that can be used together to reduce cyber risks; 3) Establishment of international agreements and frameworks that regulate the responsibilities and actions of countries in dealing

with cyber threats; 4) Training and education for workers working in the fields of information technology and cyber security. The two factors that can influence the success of cooperation between countries in dealing with cyber threats and national security challenges in the digital era include: 1) Trust and willingness to share information and technology between the countries involved; 2) Differences in approaches, policies, and laws that affect cyber security in each country; 3) Political and geopolitical factors that can influence cooperation and trust between countries; 4) Ability and availability of resources to implement the necessary cyber security measures. The three impacts of ongoing cooperation between countries in dealing with cyber threats and national security challenges in the digital era on global security and international stability include: 1) Increasing the ability of countries to deal with complex and detrimental cyber threats; 2) The formation of international frameworks and agreements that can help regulate cyber security measures and encourage cooperation between countries; 3) Increasing trust between countries in dealing with cyber security threats and increasing international stability. 4) Reducing the risk of conflict and security escalation that can arise from cyber attacks or misinterpreted cyber security measures.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Ahyati AI, Dewi DA. Implementation of National Defense in the Technology Era in Civic Education Learning. J Educ. 2021;3(3):236-47.
2. Anwar S. Mastery of Defense Technology by Indonesian Defense Human Resources in Facing Future Wars. J Def Natl Def. 2018;5(1):15-34.
3. Babys SA. Cyber War Threats in the Digital Era and Indonesian National Security Solutions. Oratio Directa. 2021;3(1).
4. Cahyono EA, Sutomo N, Hartono A. Literature review; writing and compilation guide. Nurs J. 2019;12(2):12-2.
5. Chotimah HC. Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency. J Polit Dyn Domest Polit Probl Int Relat. 2019;10(2):113-28.
6. Gasparyan AY, Ayvazyan L, Blackmore H, Kitas GD. Writing a Narrative Biomedical Review: Considerations for Authors, Peer Reviewers, and Editors. Rheumatol Int. 2011;31:1409-17.
7. Hajiansyah PP, Maulana I. United States Intervention if the People's Republic of China Invades Taiwan. SSRN. 2022. Available from: https://ssrn.com/abstract=4128011
8. Harianja A, Arianto AR, Setia MCA. Implications of Cyber Warfare Between Israel, the United States and Iran Through the Olympic Game Operation Against Iran's Nuclear Program Facilities During the Mahmoud Ahmadinejad Administration: The 2010 Stuxnet Cyber War. Moestopo J Int Relat. 2022;2(2):91-117.
9. Herdanto RN. Cyber Security Policy on State Security: A Case Study of Australia in 2010-2020 [dissertation]. UPN "Veteran" Yogyakarta; 2022.
10. Irawati A, Fadholi HB, Alamsyah AN, Dwipayana DP, Muslih M. The Urgency of Cyber Law in the Life of Indonesian Society in the Digital Era. In: Proceeding of Conference on Law and Social Studies. 2021 Aug.

11. Khoironi SC. The Influence of Cybersecurity Culture Training Needs Analysis as an Effort to Develop Competence for State Civil Apparatus in the Digital Era. J Commun Media Stud. 2020;24(1):37-56.
12. Nainggolan PP, Muhamad SV, Hidriyah S. International Cooperation Against Terrorism. Indonesian Obor Library Foundation. 2019.
13. Nastiti NN, Djemat YO, Dwiprigitaningtias I. Challenges in Implementing Anti-Terrorism Cooperation Between Indonesia and Australia 2007-2016. Glob Dyn J Int Relat. 2017;2(02):68-112.
14. Nenden E. Legal review of the determination of Locus Delicti by the police in the investigation of Cyber Crime [dissertation]. UIN Sunan Gunung Djati Bandung; 2020.
15. Rahmawati C. Challenges and Threats to Indonesian Cyber Security in the Era of Industrial Revolution 4.0. In: Proceedings of the National Seminar on Science, Technology and Innovation of Indonesia (SENASTINDO). 2020 Nov;2:299-306.
16. Rizaldi A. Development of Indonesian Cyber Security in an Effort to Face Cyber Crime Threats Through the National Cyber and Crypto Agency (BSSN) [dissertation]. University of Muhammadiyah Malang; 2022.
17. Rizki M. Development of Indonesia's Cyber Defense/Security System in Facing the Challenges of Technology and Information Development. Politeia J Polit Sci. 2022;14(1):54-62.
18. Rukin SP. Qualitative research methodology. Ahmar Cendekia Indonesia Foundation. 2019.
19. Sudarmadi DA, Runturambi AJS. Strategy of the National Cyber and Crypto Agency (BSSN) in Facing Cyber Threats in Indonesia. J Natl Resil Strateg Stud. 2019;2(2):157-78.
20. Sulistianingsih D. The Use of Online Dispute Resolution (ODR) in Dispute Resolution Through Arbitration in Indonesia. Law Polit Var Perspect. 2022;1.
21. Triwahyuni TA, Wulandari DA. United States Cyber Security Strategy. JIPSI J Polit Sci Commun UNIKOM. 2017;6.
22. Yanuarti I, Wibisono M, Midhio IW. Indo-Pacific Cooperation Strategy to Support National Defense: Indonesian Perspective. Univ War Strategy. 2020;6(1).
23. Yudistriansyah A, Suryanegara M, Gunawan D, Arifin A, Krisnadi I. Evaluation of Security Maturity Level and Recommendations for Improving Internet of Things (IOT) Security of PT XYZ Based on the IOT Security Maturity Model Framework. Univ Indonesia. 2019;1-2.
24. Yusuf SA, Khasanah U. Literature Review and Social Theory in Research. Islam Econ Res Methods. 2019;80:1-23.