ISSN 2615-3718 (Online)
ISSN 2621-5675 (Print)

Asian Institute of Research
Journal of Social and Political Sciences
Vol. 6, No.4 December 2023

Journal of Social and Political Sciences

Shiddique, M. R., & Juned, M. (2023). Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020). *Journal of Social and Political Sciences*, 6(4), 215-224.

ISSN 2615-3718

DOI: 10.31014/aior.1991.06.04.457

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.6, No.4, 2023: 215-224
ISSN 2615-3718

DOI: 10.31014/aior.1991.06.04.457

Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)

Muhammad Rafi Shiddique[1], Mansur Juned[2]

[1,2] Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

Correspondence: Mansur Juned. Email: mansurjuned@upnvj.ac.id

Abstract
The rapid development of technology poses threats in cyberspace, including in Indonesia. This type of threat is relatively new to Indonesia, especially since 2020. One of the challenges faced by Indonesia in dealing with cyber threats is the need for more competent human resources. In 2018, Indonesia and Australia collaborated in the form of the Indonesia-Australia Cyber Policy Dialogue, one of which is Capacity Building and Strengthening Connection. This research aims to discover how the Indonesian government, through BSSN, improves human resources by cooperating with Australia. The author uses a qualitative approach and descriptive research type in this research. The author also uses the concepts of international cooperation and cybersecurity to analyze this problem. The results of this study show that through BSSN, Indonesia has great potential to improve national cyberspace because it gets direct knowledge and practice from Australia. The potential of BSSN is expected to answer the need for more competent human resources in Indonesia to secure national cyberspace.

Keywords: BSSN, Capacity Building and Strengthening Connection, Indonesia-Australia Cyber Policy Dialogue

1. Introduction

Indonesia is experiencing rapid development of information technology and internet advancement. This development has reached the easy access stage for the public to the internet. This ease of access has resulted in a change in the pattern of activities of Indonesian citizens who previously had no internet intervention. Only armed with devices in their hands and connected to the internet Indonesians can carry out their activities more quickly. Based on the survey results of the Indonesian Internet Service Providers Association (APJII) in the first quarter of 2019, it was recorded that the number of internet users in Indonesia touched 196.7 million people or equivalent to 73% of the total population of Indonesia, until the second quarter of 2020. This number has increased by 64.8% from 2018.

Along with the rapid penetration of the internet in Indonesia, security in the scope of cyberspace is increasingly vulnerable. This threat can attack individuals, companies, and government institutions. This phenomenon has made the conversation about cybersecurity rise to the surface. Globalization and the internet have greatly influenced individuals, organizations, and even countries in the form of extraordinary power (Geers, 2011). Due to the vastness of space and easy access to cyberspace, traditional actors can interact in cyberspace. Since cybersecurity is linked to traditional information, the ability of states to secure the cyber world will determine their national security in the real world (Juned et al., 2023).

The National Cyber and Crypto Agency (BSSN) found that the number of cyberattacks in 2020 reached 495.3 million cases. This figure has increased by 41% from 290.3 million cases in 2019. Similarly, the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri) noted increased reports of cybercrime cases. In 2019, there were 4,586 police reports filed through the Cyber Patrol website, which is the Bareskrim Polri website for reporting cybercrime. This number has increased from 2018, which amounted to 4,360 reports. In May 2020, the Indonesian public was shocked by the news that 91 million Tokopedia accounts were successfully hacked and traded on dark websites. The leak of Tokopedia user data in the form of user ID, email, full name, date of birth, gender, telephone number, and user password. It is known that the number of active Tokopedia users is around 91 million. Almost all Tokopedia user data has been successfully hacked (Franedya, 2020).

Meanwhile, from January to July 2021, cyber attacks in Indonesia have touched 741.4 million cases, where the most common attack categories include malware, denial of service (DoS), and trojan activity. The cybercrime trend throughout the year was dominated by ransomware and index data leaks. During this period, the government sector experienced the highest data leakage due to information-stealing malware at 45%, followed by the financial sector (21.8%), telecommunications (10.4%), law enforcement (10.1%), transportation (10.1%), and state-owned enterprises (2.1%) (Badan Siber dan Sandi Negara, 2021).

The Indonesian government has tried to establish international cooperation with other countries that are stronger and more capable of handling cyber security. Indonesia cooperates with Australia in the Indonesia-Australia Cyber Policy Dialogue. Indonesia and Australia affirmed their commitment to openness, freedom, and security in cyberspace. The two countries also decided to strengthen cooperation in protecting cyberspace. The first Indonesia-Australia Cyber Policy Dialogue was held on Thursday, May 4, 2017. The dialogue was held based on cooperation, openness, and a common goal of improving the protection of cyberspace. Both sides discussed issues in cyberspace, including each country's vision of cyberspace, exchanging views on cyber threats, policies and strategies, and regional and international developments. Further discussion on potential bilateral cooperation to promote a safe and open internet for social and economic development.

Paragraph 2 of the Areas of Cooperation of the Indonesia-Australia Cyber Policy Dialogue MoU states that the two countries agreed to cooperate through Capacity Building and Strengthening Connections. The cooperation includes three concrete steps both countries will take to strengthen their cyber security. The four points include: participating countries will support skills and knowledge in cybersecurity and cyber policy through short-term programs and long-term awards (including scholarships for master's and Ph.D. programs), participating countries will explore research institutions and universities to strengthen teaching and research outcomes in cyber affairs, participating countries will explore opportunities to promote international law, norms, and responsible behavior in cyberspace.

2. Method

This research uses a non-reactive methodology. This research design will process data from reliable sources, both primary and secondary data, and analyze it using theories or concepts that have been determined to answer the problem formulation. This method will analyze primary and secondary data from literature studies to examine cooperation between Indonesia and Australia in implementing capacity building and strengthening connections in the Indonesia-Australia Cyber Policy Dialogue cooperation in 2018-2020. Primary and secondary data were collected and evaluated in this study. Data were collected using literature review, documentation, and interviews.

As a source of documentation, the researcher will collect relevant documents, including confidential records such as engagement letters and case reports to support data for study analysis and public materials such as newspapers, reports, and other public documents such as news articles. Thus, the researcher obtained comprehensive details on the issues in this study related to the two data collection procedures mentioned above. Data from the literature review and documentation were selected as guidelines and foundation in this research. All data collected will be selected or minimized using qualitative data analysis. The researcher also interviewed the Director of Cyber and Crypto Security Strategy, Sigit Kurniawan, as a form of data collection technique.

Data reduction is used to direct and classify data into information that can be used to conclude. Researchers will conduct a selection process for data from the field by collecting and sorting data based on the same or different questions and answers (Miles & Huberman, 1992).

2.1. Concept

K.J. Holsti states that international cooperation is an interaction and transaction between countries in the international system that is routine and tends to be free from conflict. Various problems that arise from the national, regional, and global scope require the attention of various countries. In some cases, governments between countries communicate with each other by proposing alternative solutions, negotiations, or dialogues related to the problems at hand, submitting various technical evidence to support the solution of specific problems, and ending negotiations by forming agreements that satisfy all parties (Holsti, 1992).

The term "security" is a controversial concept. Its traditional definition has been contested, and the concept has been the subject of various interpretations. The redefinition and expansion of the security concept in academic discussions have accompanied the development of new conceptual tools in the security research literature. The concept of "human security," which provides an alternative approach to rethinking security by emphasizing the threats and security of individuals and communities, has gained much credence in light of emerging threats and uncertainties (Emmers, 2016). Michael Smith, in his book entitled Research Handbook on International Law and Cyberspace, explains that cyber threats can come from governments, specific organizations, entrepreneurs, and individuals who have goals to gain benefits such as financial, military, political, etc. (Smith, 2015).

Cybersecurity terminology can be used in the context of national security. Even if necessary, it can use military force (Indrawan, 2019). Because it concerns national interests, cybersecurity urgently requires a series of strategies to ward off threats. Solange Ghernaouti, in her book entitled "Cyber Power: Crime, Conflict, and Security in Cyberspace," says that the development of information technology has also had a significant impact on changes related to the concept of security, changes that now allow interaction space to not only be limited physically but also extend to the cyber world. This development makes the state adapt because it is time for the cyber security concept to be established as a country's 'territory' as the state must protect its territory (Ghernaouti, 2013). With some explanations and definitions, researchers use cyber security to answer how to implement capacity building and strengthen connections in the Indonesia-Australia Cyber Policy Dialogue cooperation for 2018-2020. Therefore, this concept will find out what has been obtained by BSSN in improving the quality of Human Resources (HR) to improve national cyber security.

3. Result and Discussion

As a virtual sphere connecting various actors across national borders, cyberspace has changed the shape of contemporary international relations and posed a challenge to decision-makers and international relations academics (Juned et al., 2022). Until now, there has still been no binding international cybersecurity agreement, so Indonesia needs to take the initiative to seek such an agreement. Therefore, the absence of a binding international agreement requires Indonesia to strengthen national cyber security. Various forms of national cyber security cooperation can be reviewed through various sides, ranging from facilities and infrastructure to capacity building of human resources in maintaining national cyber security. This cooperation can be done with two countries or bilaterally. Indonesia needs to play an active role in encouraging the creation of a joint agreement in its membership in international forums (Adriyanti, 2014).

Regarding capacity, Indonesia is still a country with high cyber vulnerability. The Indonesian government needs to develop strong cyber resilience, including improving infrastructure, internet devices, and networks, as well as cyber diplomacy to boost the preparation of laws and advocacy of international norms that support the behavior of responsible states and institutions in cyberspace (Fitriani, 2019). Regulating cyberspace has become a matter of great urgency because the interconnected work mechanism makes cyberspace vulnerable. Indonesia needs to make the issue of cyber threats a top priority in the national security agenda to protect critical infrastructure and the public as internet users.

In the policy sector, concerns about cyber crime in Australia were initially set out in the Howard Government's 2000 Defense White Paper, Defence 2000: Our Future Defence Force. Some initiatives stemmed from this policy, including cooperation among national security Agencies to address emerging cyber threats. In the 2009 Defense White Paper, Defending Australia in the Asia Pacific Century: Force 2030, the Kevin Ruud Government placed cyber threats as one of its national security priorities and, in 2010, established the Cyber Security Operations Center (CSOC) under the Defence Signals Directorate. In 2013, under the Julia Gillard government, the CSOC evolved into the Australian Cyber Security Centre as the "hub of the government's cyber security efforts." The 2013 Defence White Paper recognized that dealing with cyber threats requires a whole-of-government approach and industry engagement.

Australia and Indonesia's cybersecurity issues have led both countries to view cybercrime as a transnational crime threatening national security. This common perception gives Australia and Indonesia a collective identity as countries that suffer from being targeted by cybercrime and have become countries that have begun to focus on strengthening cybersecurity. This identity, fueled by similar perceptions, has led both countries to work to address cybersecurity to create cybersecurity in both countries. This is the answer to understanding the two countries' behavior in the similarity issue. Even with the background of crisis-ridden and dynamic relations between the two countries, a new approach to understanding security cooperation between the two countries can be based on the possibility of creating common interests to deal with global problems faced by the people of both countries (Tanther, 2012).

3.1. Cyber Bootcamp

The cyber boot camp is a project under DFAT's Cyber Cooperation Program. The program is a form of collaboration between Australia and partner countries across the Indo-Pacific to improve cybersecurity. Established in 2016, the Cyber Partnership Program is crucial in supporting Australia's participation in cyberspace to promote a free, open, and secure Internet that protects national security and promotes international stability while driving global economic growth and sustainable development. (Australian National University, 2019).

BSSN, as DFAT's cybersecurity cooperation partner, also conducted this Cyber boot camp activity. A cyber boot camp is an activity that provides training and learning for BSSN delegates and other stakeholders who participate in this type of camp. This activity aims to build participants' knowledge and awareness of technology readiness, cyber threats, decision-making, and the nature of cyberspace.

The cyber boot camp is an intensive two-week program in Australia. Participants participate in workshops, training, industrial park tours, and dialog with Australian government agencies in this activity. With this activity, Australia hopes the participants will conduct training and learning to respond to relevant cyber threats in Indonesia and help strengthen cybersecurity in the Indo-Pacific.

Cybersecurity collaboration with Australia through the Cyber boot camp program launched by the National Cyber and Crypto Agency (BSSN) is an essential strategy that has significant potential to strengthen the ability of the Indonesian people to face global cyber threats in the field of cybersecurity. Cyber boot camp is an intensive training program that teaches delegates about cybersecurity, the latest technology, decision-making related to threats faced, and safe hacking of computer networks. Delegates can participate in workshops, courses, and ongoing discussions with Australian government agencies. For Indonesian human resources, including BSSN, this strengthens their ability to navigate the national cyber defense system. The knowledge and skills developed from this program can be leveraged to strengthen Indonesia's cyber system.

The Cyber boot camp program, a form of cooperation between Indonesia and Australia Cyber Policy Dialogue, reflects a joint commitment to improve cybersecurity at the Indo-Pacific level, not only at the Indonesian national level. This cooperation is an excellent concrete example of regional cooperation in dealing with cyber threats with a variety of knowledge, experience, and practices provided. Indonesia has the opportunity to expand its cybersecurity network across the region and strengthen its position as an important player in global cybersecurity. Cyber boot camps can contribute to the strengthening of bilateral relations between Indonesia and Australia. Both countries are interdependent in dealing with cyber threats, and cooperation can strengthen ties in many other areas. This includes economic cooperation, trade, and diplomacy related to cybersecurity.

Sigit Kurniawan, Director of Cyber and Crypto Security Strategy at the National Cyber and Crypto Agency (BSSN), continued that the cyber boot camp has been held regularly every year since 2018. In this cyber boot camp activity, delegates from Indonesia, including BSSN, will get materials for improving cybersecurity. Sigit Kurniawan said the material is in the form of cybersecurity policymaking. During the cyber boot camp program, participants will learn how Australia implements its national cyber security.

In addition to providing material, Sigit Kurniawan also stated that one of the cyber boot camp series was a visit to the Australian Cyber Security Center (ACSC), Australia's cyber security agency. In addition to the visit to ACSC, the Indonesian delegates, including BSSN, also visited several other institutions involved in implementing Australian cyber security. The purpose of the visit, Sigit Kurniawan continued, was to find out how Australia implements its national cyber security and how collaboration between government institutions and the private sector in dealing with cyber threats.

The series of cyber boot camps conducted by Indonesian delegates, including BSSN, has the potential to positively impact the strengthening of human resources in Indonesia related to tackling cyber threats. Australia's measures, including the applicable cybersecurity policies, can provide Indonesia with additional insights into strengthening cybersecurity, according to Sigit Kurniawan.

Through this cyber boot camp, ANU Cyber Academy CEO Dr. Lesley Seebeck said the activity focused on developing the delegates' skills to understand better how to build, construct, and maintain security networks to prevent cyber attacks. Australia has also designed the camp to bring together the skills and expertise of the delegates, who will extend their expertise to government, academia, and the private sector. According to a KOMINFO report, Indonesia needs more human resources in cybersecurity and at least 1,000 experts in this field. Therefore, this cyber training program is expected to make up for Indonesia's need for more human resources in cybersecurity.

Director of Cyber and Crypto Security Strategy of the National Cyber and Crypto Agency (BSSN), Sigit Kurniawan, assessed that the performance of Indonesian Human Resources (HR) in tackling global cyber threats has been qualified. However, he said that the cooperation between Indonesia and Australia through the Indonesia-Australia Cyber Policy Dialogue, one of which is in the form of Cyber Bootcamp, is still essential because Indonesia needs to get more insight from other countries with more qualified human resources in securing cyberspace.

The cyber boot camp provides delegates, mainly from BSSN, with a better understanding of the latest technology and challenges to be faced in cybersecurity. This can significantly boost their efforts to protect national critical infrastructure, including the security of citizens' data. Delegates with knowledge and experience are expected to be an excellent opportunity to strengthen cybersecurity in Indonesia.

Sigit Kurniawan continued handling the country's cyber security; efforts must be made in capacity building supervision so that the cyber boot camp, according to Sigit Kurniawan, must be carried out. Although this cooperation has great potential, several things need to be considered. One of them is adequate supervision and policy to ensure that the knowledge gained by the delegates, including BSSN obtained in the Cyber Bootcamp, is applied and provides tangible benefits in dealing with cyber threats in Indonesia.

The cyber boot camp program has excellent potential to strengthen Indonesia's cyber security. Cybersecurity involves using secure technology and a deep understanding of threats, responses, and effective policies. The cyber boot camp provides an essential foundation for understanding the concept of cybersecurity by focusing on several key aspects. One of these is the understanding of threats. Cybersecurity is concerned with the identification, evaluation, and mitigation of potential threats that may occur in cyberspace. The Cyber Bootcamp gave delegates a better understanding of the various cyber threats, ranging from state cyberattacks to the commercial sector. This knowledge allows BSSN to develop more effective strategies in dealing with cyber threats.

Cybersecurity is constantly evolving along with technology. The Cyber boot camp provides an opportunity to keep abreast of the latest technological developments in cybersecurity. Delegates can learn and implement the latest security solutions to protect the country's critical infrastructure and the personal data of Indonesian citizens. Success in cybersecurity depends on technology and infrastructure readiness. Through Cyber boot camp, delegates can understand the extent to which the technology used in Indonesia is adequate to deal with global cyber threats. They can improve infrastructure and enhance technology readiness to reduce cybersecurity risks.

Decision-making is critical in cybersecurity in making quick and appropriate decisions in the face of cyber threats. Cyber boot camp delegates received training in decision-making related to cybersecurity. This capability is critical in responding to attacks and maintaining national cybersecurity. The Cyber boot camp can also help Indonesia formulate and implement more effective cybersecurity policies. Delegates can gain insight into the best practices that Australia has implemented and apply them at the national level. Cooperation with Australia in the Cyber boot camp can also assist Indonesia in formulating and implementing a more effective cybersecurity policy. Delegates can gain insight into the best practices implemented in Australia.

With an increased understanding of cybersecurity concepts, improved technological capabilities, and improvements in decision-making and cybersecurity policy, Indonesia has an excellent opportunity to strengthen its cyber understanding. More vital cybersecurity will help protect Indonesia's critical infrastructure, citizens' data, and national interests from increasingly complex global cyber threats (Putra et al., 2018). The Cyber boot camp program with Australia creates a valuable opportunity to strengthen Indonesia's cybersecurity by improving technological understanding, decision-making, and cybersecurity policy. With a more solid cybersecurity concept, Indonesia is expected to protect itself from global cyber threats more effectively.

3.2. Australian Strategic Policy Institute (ASPI) Cyber Workshop

ASPI aims to organize workshops on responsible state behavior in cyberspace for Australia's cybersecurity partner countries. ASPI also works with BSSN to improve cyber threat analysis, engage on network policy issues, and coordinate across government agencies.

This activity took place on November 1, 2018 in Jakarta. The material was related to cyberspace and cybersecurity, risk management, risk strategy and control, cybersecurity and software security, and security architecture. In cyberspace risk management, threats can be divided into two: intentional and unintentional; for example, intentional threats are criminal acts and terrorist acts that will have social, economic, political, and government impacts. With the ASPI Network Policy Workshop activities, Indonesia, which still needs appropriate action in risk management in the field of cybersecurity, will be able to strengthen further the analysis of cyber threats that still occur frequently in Indonesia. Risk management is a fundamental element of strategy. From the risk management, the required budget can be calculated (Magrisa & Fuadi, 2020).

In the fight against cyberattacks, a lot of money is spent to ensure the security of a country's information and data. Thus, strategic risk management makes countermeasures against cyberattacks more affordable. In addition, through ASPI's Cyber Policy Workshop, it is hoped that stakeholders in the field of cyber security in Indonesia can coordinate and collaborate to address cyber threats and improve cyber security with strategic steps.

Through cooperation with ASPI, Indonesia can strengthen its national cybersecurity efforts. This will help the country deal with increasingly complex cyber threats, both intentional and unintentional. Indonesia is also expected to be able to identify various types of threats with a deeper understanding of cyber threats so that countermeasures can be formulated more effectively. The ASPI Cyber Workshop can assist Indonesia in formulating more robust cybersecurity policies and strategies. This involves the development of a comprehensive risk management framework, which enables the identification, evaluation, and mitigation of risks in cyberspace.

3.3 Cyber Security Webinar

As a form of implementing Capacity Building and Strengthening Connections in the Indonesia-Australia Cyber Policy Dialogue collaboration, webinars were held from 2020 to 2021. Sigit Kurniawan said that the webinar held in this collaboration invited experts in cybersecurity from various parties, from the government to the private sector from Australia.

The topics carried out in this webinar depart from the agreement obtained between Indonesia and Australia. Sigit Kurniawan said that technology management was one of the topics discussed in the Capacity Building and Strengthening Connection webinar. On this topic is the response of a country, especially Australia, in responding to the presence of 5G Internet, the Internet of Things (IoT), and the rise of the phenomenon of artificial intelligence (AI), which has recently often been discussed and widely used by the wider community. Sigit Kurniawan continued that the webinar discussed what policies related to cybersecurity Indonesia and Australia have in responding to the presence of technological advances.

Apart from discussing the theme of technology management, Sigit Kurniawan added that the webinar, which was held as a form of Capacity Building and Strengthening Connection Indonesia-Australia Cyber Policy Dialogue, also raised the issue of technical aspects, computer science, and network security.

In the webinar, there was a dialog session where Indonesia and Australia presented data related to the phenomenon that was the topic of discussion. Sigit Kurniawan said that in this session, the two countries provided each other's perspectives regarding data on a phenomenon that is the topic of discussion. In this session, one party can ask for a comprehensive explanation from the other party involved regarding their steps towards the cyber phenomenon being discussed. For example, in the webinar session, Sigit Kurniawan said Indonesia could ask Australia to explain its steps in protecting its citizens' data.

The webinar within the Indonesia-Australia Cyber Policy Dialogue cooperation framework has provided a strong foundation for strengthening cyber security in Indonesia. Through an in-depth approach to cybersecurity, Indonesia, through BSSN, can develop a more holistic strategy for protecting its digital infrastructure. However, Indonesia is also faced with some significant challenges that need to be overcome, including limited resources and low public awareness of cybersecurity.

In addressing these challenges, Indonesia can continue to leverage its cooperation with Australia but must also take internal initiatives to strengthen its cybersecurity capacity. This includes stronger policy-making, continuous education and training, and more effective law enforcement related to cybersecurity. By doing so, Indonesia can strengthen and maintain better cybersecurity in the future.

One of the aspects emphasized in the cybersecurity webinar was the concept of deep cybersecurity. Deep cybersecurity is a comprehensive approach to protecting data, networks, and digital infrastructure. It includes robust technology and software, sound risk management principles, user awareness, and cross-sector cooperation. In this case, through BSSN, Indonesia can cooperate with Australia to develop the concept of deep cybersecurity in line with the rapid development of technology.

BSSN is the state agency responsible for cybersecurity policy and implementation in Indonesia. BSSN plays a central role in ensuring cybersecurity in the country. Based on some webinars within the framework of the

Indonesia-Australia Cyber Policy Dialogue cooperation, BSSN has an excellent opportunity to strengthen Indonesia's cybersecurity and develop cybersecurity policies and practices in Indonesia.

BSSN can utilize the knowledge gained from these webinars to develop more substantial and more sustainable cybersecurity policies. Various regulations and guidelines will help Indonesia deal more effectively with cyber threats, regulate the use of the latest technologies such as 5G, the Internet of Things (IoT), and artificial intelligence, and safeguard the Privacy of every citizen. Some webinars that have been held can also be utilized by BSSN in developing security standards that align with the latest technological developments. In addition, cybersecurity certification can be introduced to incentivize organizations in Indonesia to improve cybersecurity.

Human Resources (HR) is a valuable asset in cybersecurity. Training and developing the workforce in cybersecurity is an essential step in dealing with increasingly complex threats (Rohmah, 2022). One of the challenges now felt in cybersecurity in Indonesia is the need for adequate human resources. The need for qualified human resources in cybersecurity is a severe problem in terms of cybersecurity (Yunita, 2016). Some webinars in the Indonesia-Australia Cyber Policy Dialogue cooperation have provided essential insights for Indonesia, especially BSSN, which can be applied to strengthen human resources in Indonesia in cybersecurity. Training and certification are effective ways to improve cybersecurity. BSSN can collaborate with educational and training institutions to organize training programs by international standards. Certification can also provide legitimacy to cybersecurity professionals in Indonesia.

Cybersecurity covers various disciplines, including technology management, computer science, networking, and policy. BSSN can identify areas for improvement and support education programs that focus on specific skills. This will help Indonesia produce experts capable of addressing the increasingly diverse cyber threats. Cybersecurity is a constantly evolving field, with new attacks emerging every day. BSSN can support research and innovation in cybersecurity by establishing partnerships with universities and research institutions. This will help Indonesia develop creative and adaptive solutions to global cyber threats.

4. Conclusion

Cooperation in the cyber field between Indonesia and Australia is related to the cyber policy dialogue program between the two countries called the Indonesia-Australia Cyber Policy Dialogue. Paragraph 2 of the Areas of Cooperation of the Indonesia-Australia Cyber Policy Dialogue MoU states that the two countries agreed to cooperate through Capacity Building and Strengthening Connections. The cooperation includes three concrete steps to be taken by both countries in strengthening their perspective regarding cyber security.

Australia and Indonesia reaffirm their approach to an open, accessible, and secure cyberspace for economic growth and innovation, and they commit to strengthening partnerships to combat cyber threats. They committed to working with other regional partners to reduce the risk of cyber threats. The two countries agreed that the cybersecurity policy dialog has formed a solid foundation for future partnerships. The two sides discussed various cyberspace topics, including different visions of the Internet and cyberspace, cyber threat perceptions, policies, strategies, and regional and international trends. Discussions also focused on possible bilateral cooperation to promote a safe, open, secure Internet for economic and social development. Indonesia – Australia Cyber Policy Dialogue presents some hefty possibilities for Indonesia's cyber growth, including the possible growth of Human Resources capacity. The enhanced understanding of cyber security players and the ability to recognize early threats are good elements that Indonesia obtained from Australia due to the established collaboration.

Implementing the Capacity Building and Strengthening Connection in the Indonesia - Australia Cyber Policy Dialogue provides essential insights into increasing the knowledge of human resources in Indonesia, especially BSSN, to strengthen national cyber security. BSSN can utilize the knowledge gained from Australia, both when visiting institutions in Australia that play a role as cybersecurity actors and in the form of boot camps or webinars held. A series of knowledge gained from implementing the Capacity Building and Strengthening Connection can be utilized by BSSN in preparing itself to face the challenges of cyber threats in Indonesia that will come and those that have often occurred.

One of the challenges now felt in cybersecurity in Indonesia is the need for adequate human resources. The need for qualified human resources in cyber security is a severe problem in terms of cyber security. HR advancement plays a vital role in securing Indonesia's cyberspace, including protecting critical infrastructure and the security of citizens' data. The Capacity Building and Strengthening Connection Indonesia-Australia Cyber Policy Dialogue is fresh air for developing cybersecurity human resources in Indonesia. Establishing this collaboration opens opportunities for Indonesia through BSSN to increase human resources capacity to strengthen cybersecurity.

Author Contributions: All authors contributed to this research.

Funding: Not applicable.

Conflict of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics Approval: Not applicable.

References

Adriyanti, H. (2014). Cyber Security and its Development Challenges in Indonesia. *Jurnal Politica*, *5*(1), 95–110. http://dx.doi.org/10.22212/jp.v5i1.336

Australian National University. (2019). *Cyber Bootcamp Project kicks-off with Indonesian partners*. Australian National University. https://nsc.crawford.anu.edu.au/department-news/15649/cyber-bootcamp-project-kicks-indonesian-partners

Badan Siber dan Sandi Negara. (2021). *Annual Report: Monitoring State Cybersecurity*.

Emmers, R. (2016). *Non-Traditional Security In Asia: Dilemmas In Securitization*. Routledge.

Fitriani. (2019). *Seeking a Common Understanding of Cyber Security in Indonesia dalam Towards Resilient Regional Cybersecurity: Perspective and Challenges in Southeast Asia*. Center for Strategic and International Studies in Indonesia.

Franedya, R. (2020). *91 Million User Data Leaked, Tokopedia Sued for 100 M*. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m/2

Geers, K. (2011). *Strategic Cyber Security*. NATO Cyber Defence Centre of Excellence.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict, and Security in Cyberspace*. EPFL Press.

Holsti, K. J. (1992). *International Politics: An Analytical Framework*. Binacipta.

Indrawan, J. (2019). *Introduction to Security Studies*. Intrans.

Juned, M., Bainus, A., Saripudin, M. H., & Pratama, N. (2022). The Dynamics Of The USA And China Relations In The Cyberspace: Struggle For Power In A Global Virtual World In Building A Global Cyber Regime. *Inderscience Online*, *30*(3–4), 396–414. https://doi.org/10.1504/IJBG.2022.123617

Juned, M., Maryam, S., Salam, S., & Utami, R. A. A. (2023). TikTok's Conflict of Interest with the US Government: Between Big Data Security and Economics (2017-2023). *European Journal of Communication and Media Studies*, *2*(4), 1–8. 10.24018/ejsocial.2023.2.4.23

Magrisa, D., & Fuadi, A. (2020). COOPERATION BETWEEN INDONESIA'S STATE CYBER AND CIPHER AGENCY (BSSN) AND AUSTRALIA'S DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT) IN DEVELOPING CYBER SECURITY. *JOM FISIP*, *7*(2), 1–11. https://jom.unri.ac.id/index.php/JOMFSIP/article/view/29009

Miles, M. B., & Huberman, A. M. (1992). *Qualitative Data Analysis*. UI Press.

Putra, R. D., Supartono, & Deni. (2018). Cyber Threats in the Perspective of Universal Defense. *Jurnal Prodi Perang Asimetris*, *4*(2), 99–120. https://doi.org/10.33172/pa.v4i2

Rohmah, R. N. (2022). Efforts to Build Cybersecurity Awareness among E-commerce Consumers in Indonesia. *Jurnal Cendekia Niaga*, *6*(1), 1–11. https://doi.org/10.52391/jcn.v6i1.629

Smith, M. (2015). *Research Handbook On International Law And Cyberspace*. Edwar Elgar Publihsing Limited.

Tanther, R. (2012). Shared problems, shared interests: reframing Australia-Indonesia security relations. In J. Purdey (Ed.), *Knowing Indonesia: Intersections of Self, Discipline and Nation* (Vol. 1, pp. 123–156). Monash University Press.

Yunita. (2016, December 27). *Indonesia lacks Cyber Security Talent*. Kementerian Informasi Dan Komunikasi. https://www.kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media