The Role of Indonesia's National Cyber and Crypton Agency in Dealing with the Increase in Cybercrime at the Beginning of the COVID-19 Pandemic

Dewi Triwahyuni[1*]
Department of International Relations, Faculty of Social and Political Sciences
Universitas Komputer Indonesia, Jalan Dipati Ukur 102-106, Bandung, INDONESIA
*dewi.triwahyuni@email.unikom.ac.id

Sylvia Octa Putri[2]
Department of International Relations, Faculty of Social and Political Sciences
Universitas Komputer Indonesia, Jalan Dipati Ukur 102-106, Bandung, INDONESIA
Sylvia.octa.putri@email.unikom.ac.id

Farhan Salim Nurjati[3]
Department of International Relations, Faculty of Social and Political Sciences
Universitas Komputer Indonesia, Jalan Dipati Ukur 102-106, Bandung, INDONESIA
Farhan.44320029@mahasiswa.unikom.ac.id

ABSTRACT

This research aims to create a sense of humanity to unite people to help each other deal with the COVID-19 disease outbreak, which has now developed into a pandemic. Amid the global fight against COVID-19, cybercriminals are exploiting the negligence of various parties for financial gain. In today's information era, information is crucial, and the internet, despite its benefits, is also prone to misuse for cybercrime. The COVID-19 pandemic has led to a surge in cybercrime cases. Cyberattacks increased sharply in 2020, dominated by trojan activities and data collection. The government seeks to address this cybercrime threat through the National Cyber and Crypto Agency/"*Badan Siber dan Sandi Negara"* (BSSN). This study aims to examine the increase in cybercrime during the pandemic and the role of the National Cyber and Crypto Agency in dealing with it.

Keywords: *BSSN, Covid-19 Pandemic, Cybercrime, Indonesia's cyber security*

L. Warlina and S. Luckyardi (eds.), *Proceedings of the International Conference on Business, Economics, Social Sciences, and Humanities - Humanities and Social Sciences Track (ICOBEST-HSS 2024)*, Advances in Social Science, Education and Humanities Research 854,
https://doi.org/10.2991/978-2-38476-269-9_3

1. INTRODUCTION

In the information age, the existence of information has a vital role in aspects of life. Information is also one of the necessities of life for everyone, both individuals and organizations, so information functions like the blood flow of life sources for humans. One of the findings that has significantly impacted the information society is the internet. The internet, as a new form of technology, causes humans to be unable to escape the flow of communication and information. Like any other technology, the Internet has caused one giant leap in life.

Technology will be effective if we pay attention to the usefulness of technology by social and personal values and government regulations that protect society from adverse impacts. Related to the existence of the internet, there is a related concept, namely *cyberspace*. The term *cyberspace* is the digital world realized through the internet network, consisting of websites as virtual buildings, connections as roads, and users who interact in them. One of the negative impacts that arise in *cyberspace* is *cybercrime*. The increase in *cybercrime* requires more attention and seriousness in developing *cybersecurity* for the Indonesian state.

COVID-19 cases have rocked the world since the end of 2019. People are brought together by humanity to assist one another in coping with the COVID-19 disease outbreak, which has now turned into a pandemic. However, in the middle of the global effort to combat COVID-19, cyber threat actors also exploit other people's carelessness to make money. Threat actors frequently use the public's want to provide information on the origins and management of the COVID-19 outbreak as a cover for illegal incursions. Cyber fraud perpetrators typically use computer abuse tactics, such as cracking, data stumbling (diddling), and data leakage (faking), to carry out their crimes. Assault that causes a denial of service. Pretend to be someone else, fabricate and threaten emails (email fraud and trolling), and infiltrate (*piggybacking*).

The National Cyber Security Operations Center of the National Cyber and Crypto Agency/"*Badan Siber dan Sandi Negara"* (BSSN) recorded 88,414,296 cyber-attacks from January 1 to April 12, 2020. In January, there were 25,224,811 attacks; in February, 29,188,645 attacks were recorded; in March, there were 26,423,989 attacks; until April 12, 2020, there were 7,576,851 attacks. The peak number of attacks occurred on March 12, 2020, and reached 3,344,470 attacks. After that, the number of attacks decreased significantly with the implementation of work-from-*home* (WFH) policies in various places. However, during WFH, there have been cyberattacks that have taken advantage of issues related to COVID-19. The most common type of attack was *trojan activity,* as much as 56%, followed by *information gathering* activities (information gathering), as much as 43% of the total attacks, while the remaining 1% were *web application attacks* (BSSN, 2020).

In many cases above, cybercrime has increased, especially during the pandemic. The task of carrying out security against cyber threats is organized by government agencies engaged in cybersecurity, in this case, the National Cyber and Crypto Agency (BSSN). In this case, it aims to address the increase in *cybercrime* during the pandemic and find out the role of BSSN in handling it.

The study "The Threat of Cyberattacks on Indonesia's National Security" by Vimy et al. (2022) is a similar research study. In their piece, they go over how to identify priorities for mitigating cyber threats, which can then be used to strengthen Indonesia's cybersecurity. This conversation has led to some similarities in the research subject, Indonesia's cyber

security system, where researchers are searching for remedies and mitigating measures akin to averting cyberattacks on a national scale.

Cynthia Rahmawati (2020) also wrote related research on "Challenges and Threats of Indonesian Cybersecurity in the Era of Industrial Revolution 4.0". Our researchers discovered similarities in the study subject, cybersecurity in Indonesia, by examining the aspects of risks and problems closely related to evaluating the preparedness of the country's cybersecurity system. The distinguishing factor that enhances this study is the researchers' approach to broadening and deepening the subject of their investigation, reinforcing prior studies concentrated exclusively on domestic phenomena. This expansion extends their analysis into Southeast Asia, enriching the academic discourse.

2. LITERATURE REVIEW

Security is one of the ideas in international relations. Since the state is the fundamental unit of international relations (IR), the field of International Security Studies (ISS) is centered on state security, which is sometimes referred to as "national security." One of the tenets of international politics is that states seek to be secure, and security entails preserving territorial integrity and defending a specific set of political and cultural values. On the other hand, while nations agree to pursue security, they cannot agree on how this would affect war and conflict (Buzan & Hansen, 2007).

The government and its armed forces often manage security-related matters (Croft, 2006). The concept of security encompasses a range of issues about human existence, including military and social, cultural, political, and economic ones. As a result, cybersecurity becomes crucial in this situation, where national and international security that upholds human rights online is becoming more complicated and susceptible to more advanced attacks (Stevens, 2016).

Cyberspace is becoming more dangerous at a time when people rely more and more on information technology (IT). Cyberattacks on particular targets can be carried out by various entities, including states, non-state actors, groups supported by states, and individuals. Sims (2011) stated: These cyberattacks threaten corporations, society, and national security. Thus, it is critical to realize that cybersecurity is a significant problem that nations and corporations must address. Investing in security technologies, training, and developing appropriate policies and procedures is imperative to counteract increasingly sophisticated and expensive cyber threats.

Cyber-security is a set of tools, policies, security concepts, security protections, guidelines, risk management approaches, actions, training, best practices, safeguards, and technologies that can be used to protect cyber environments, organizations, and user assets. Cyber-security organizations and user assets comprise networked computers, employees, infrastructure, services, applications, and telecommunications systems, as well as the total amount of data that is transferred and/or stored in a virtual environment (Ardiyanti, 2016).

In the realm of technology and cyberspace, human presence is crucial. Many different entities, including individual hackers, criminal organizations, terrorist organizations, corporations, and nation-states, pose a threat of cyberattacks. Malicious acts can be carried out by any attacker in cyberspace. State and non-state actors are the two categories of attackers used in cyberattacks. This classification shows how parties with disparate interests and objectives might pose a threat in the form of cyberattacks. As a result, it is

critical to raise awareness of and equip ourselves to handle better the danger posed by cyberattacks from both state and non-state actors. (Lukasik et al, 2003).

3. METHODOLOGY

This research uses qualitative research methods through phenomenological research design. According to Creswell (2010), phenomenology is an approach from philosophy and psychology that describes an individual's lived experience of a phenomenon as told by the perpetrator.

The phenomenological approach is also used to analyze a phenomenon to find the best solution to unresolved problems. Phenomenology was chosen because cyber threats have existed for a long time. Their forms are growing every time, so electronic-based government systems need security through strategies made by Indonesia. Therefore, the National Cyber and Crypto Agency (BSSN), Indonesia's leading sector and cyber agency, must create a strategy to tackle these cyber threats, which are also part of a non-military threat.

The data collection techniques used in this research are semi-structured interviews, also called in-depth interviews, literature studies, and documentation. The data that has been collected is then tested for validity at the credibility stage, namely through triangulation techniques.

4. DISCUSSION

Since the end of 2019, the coronavirus case outbreak, known as COVID-19, has consumed the world. People have been eager to learn more about the origins and management of the Covid-19 pandemic ever since. Numerous neighborhood organizations have come together out of a shared sense of humanity to assist one another in containing the coronavirus epidemic, which has now spread into a pandemic. The COVID-19 pandemic occurred against the backdrop of the crisis of multilateralism. Even though global cooperation is crucial in combating the spread of the virus and in developing a vaccine, the media has depicted multilateralism as being slow to act, deficient in political leadership, and a source of disappointment for many (Triwahyuni, 2022).

Numerous cybercrimes have happened, such as online and computer assaults connected to how the government handled the COVID-19 outbreak. Recently, there has been a debate about law enforcement's role in combating cybercrime, with some claiming that there is injustice in the system. While there is optimism that the government's efforts to apply criminal law in this case will be acceptable, cybercrime is a real problem that necessitates adequate law enforcement measures in response to evolving conditions and scenarios (Ismansyah et al, 2023).

However, even as the world fights COVID-19, cyber threat actors also use other people's carelessness for their financial gain. Threat actors frequently take advantage of the community's eagerness to provide information on the origins and management of the COVID-19 epidemic to carry out.

According to data gathered by the National Cybersecurity Operations Centre (BSSN), there had been 25 cyberattacks up until April 12, 2020, with 17 targeting worldwide targets and 8 targeting specific countries. These attacks were carried out against the backdrop of the Covid-19 pandemic. Cyberattacks of the malicious email phishing kind occurred in January and February, both of which used the background of the Covid-19 pandemic issue.

With 22 cyberattacks in March, the month with the highest number was caused by the Covid-19 pandemic. These attacks included a variety of techniques, such as the use of the HawkEye Reborn Trojan, Blackwater malware, BlackNET RAT, DanaBot banking Trojan, Spynote RAT, Netwalker ransomware, Cerberus banking Trojan, Ursnif malware, Adobot spyware, Trojan Downloader Metasploit, Projectspy spyware, and Anubis banking Trojan.

In addition to cyberattacks based on the Covid-19 pandemic issue, there are also web defacement cyberattacks. This cyber attack is generally more massive on weekends and national holidays. In January, there were 16 cyber-attacks; in the first week, there were 13 attacks. In the second week, there was one attack, and in the fourth week, there were two web defacement attacks, with Mr. being the top attacker. In February, there were 26 web defacement cyber attacks: one attack in the first and second weeks, 15 in the third week, and nine in the fourth week, with SERAVO as the top attacker. In March, there were 69 cases of web defacement cyber attacks: 23 attacks in the first week, 14 attacks in the second week, 17 attacks in the third week, and 15 attacks in the fourth week, with Gse7en and Simsimi as the top attackers. In April 2020, there were 48 cases of cyberattacks; 34 occurred in the first week, and 24 others occurred in the second week of April, with Simsimi as the top attacker.

Cyber incidents include virus attacks, data theft, theft of personal information, infringement on a company's intellectual property, vandalism of websites, and difficulties accessing electronic services that interfere with the normal operation of electronic systems. Because work must be done through the network, the work-from-home mechanism raises the potential risk even more. Organizations need to take the COVID-19 epidemic seriously as a catalyst to enhance information security procedures and foresee cyberattacks. Effective planning can reduce losses resulting from data theft, service interruptions, and the spread of cyber incidents. As soon as feasible, the firm must recover its electronic systems and data harmed by the incident to continue its commercial operations. The data gathered during the incident management process can be a foundation for future incident handling planning and improvement initiatives. Evidence of cyberattack occurrences may be utilized to bolster legal action if needed.

A significant cybercrime case involving the hacking of the e-commerce platform Tokopedia occurred in March 2020, marking the start of the epidemic. It was revealed that Tokopedia had been hacked, with an estimated 91 million accounts and 7 million merchant accounts—not the 15 million previously stated. On the other hand, Tokopedia reported in 2019 that there were approximately 91 million active accounts on its network (Suyanto, 2003). This indicates that nearly every Tokopedia account has been successfully hacked. The offenders sell user IDs, emails, complete names, dates of birth, gender, phone numbers, and passwords that are still encrypted on the dark web. They were sold for US$5,000, or around IDR 74,000,000.00 (seventy-four million rupiah). Even now, 14,999,896 Tokopedia accounts have data available for download. (Tambunan et al., 2018).

From the many cases at the pandemic's beginning, BSSN divided several aspects that became the main focus in securing the system: data/information security, application security, network security, and infrastructure security. These four aspects lead to the establishment of system security standards and criteria.

Before formulating a strategy, several important things must be considered in strategic management. According to F. R. David (2011), strategic management consists of three stages: strategy formulation, implementation, and evaluation. To build a system security strategy, BSSN must undoubtedly pay attention to the vision and mission of the system, as

stated in Presidential Regulation Number 95 of 2018, which is related to electronic-based government systems. In addition, BSSN must also identify obstacles and challenges. An alternative strategy should also be developed as a backup if the first strategy cannot achieve the predetermined goals.

The second step is strategy implementation. BSSN, through Presidential Regulation No. 95, as the person in charge of system security, must implement the strategies that have been developed. However, to ensure the implementation of the strategy, BSSN must set objectives, develop policies, and allocate resources to contribute to the implementation of the strategy. All can be done if BSSN organizationally has created a culture that supports the strategy, improves work efficiency, and develops a budget structure. This is essential because it is the action step where the strategy is implemented.

The last step is strategy evaluation. This step is usually carried out by the head of the facility, in this case, the head of BSSN, to determine the security strategy implemented by BSSN. Strategic evaluation is also a step to make proposals for improving the implemented strategy to enhance the quality of the strategy in the future. As part of the system security strategy, BSSN conducts assessments to know and analyze the readiness of national system security.

BSSN releases a recapitulation report of Cyber Attacks Before and After the Pandemic in Indonesia (see Figure 1 below). Simply put, pandemics play a very active role in the increasing number of cyber attacks taking place today. At the outset of the pandemic, the increase in cyber attacks was not so rapid, but after 2021, the rise in cyber attacks would be enormous. Even the total from January 2021 to June 2021 alone is much higher than the total of previous years. After entering the pandemic period, the average every three months rises to ten times as high as before the pandemic. The graph also shows that every three months, the number of cyber attacks is increasing. The first increase that began to change was July-September in 2019, and the biggest increase occurred in April-June in 2021. Figure 1 shows a very distant difference from the pre-pandemic average of 14.087.989, whereas, after the pandemic, 156.222.597 has increased to ten times (BSSN 2019, 2020).

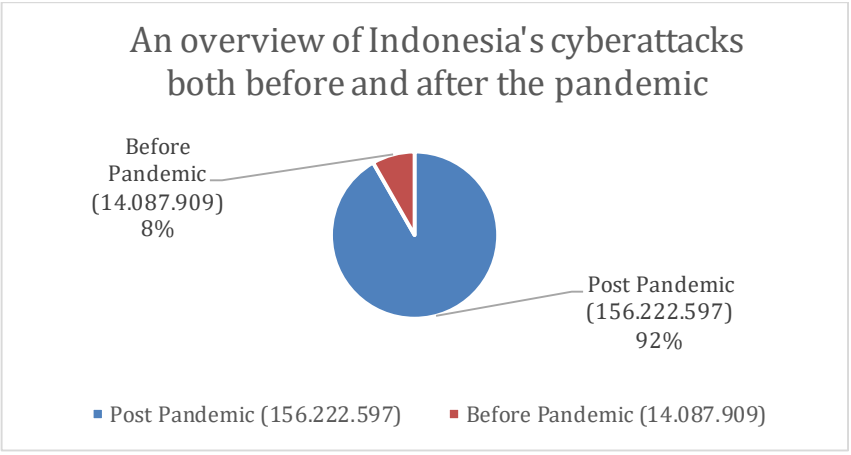

Figure 1: An Overview of Indonesia's cyberattacks both before and after the pandemic

In addition to the strategic management aspect, BSSN needs to develop a security strategy to deal with cyber threats to the system because there are still severe vulnerabilities, as previously described. Therefore, the analysis will be studied using the strategy theory proposed by Arthur F. Lykke (1998). There are three aspects to formulating a strategy: ends, means, and ways. Ends are objectives or goals to be achieved from the strategy (see Figure 1). Meanwhile, means are all the resources used and mobilized to achieve the strategy's main objectives. Then, concepts or actions are used to achieve the main goals or objectives.

Figure 2: Arthur F. Lykke's Strategy Formula

BSSN's role in securing the system certainly has its challenges, namely:

1. Availability.
   System services often require high data availability, so the challenge is to deal with attacks on data availability. This is undoubtedly related to the National Data Center and is the responsibility of the Ministry of Communications and Information Technology Indonesia. In this case, BSSN must coordinate with Komungo to check the security feasibility of building the National Data Center.

2. Data Privacy/Confidentiality.
   Some system services manage personal and valuable data. The challenge is how to secure personal data. This is also the responsibility of the Ministry of Communications and Information Technology Indonesia. as the organization responsible for data integration and interoperability as well as the utilization of the

national data center. BSSN is accountable for maintaining the data security of system users.

3. Software Patching.
   The number of system applications is divided into 2 (two), namely general applications and unique applications. In the future, an increasing number will be allocated to all government agencies; the challenge that needs to be faced is how to achieve security by patching or applying patches to each existing application. In this third point, what is needed is not only how to fix each application but also requires people who are experts in patching. Again, the workforce is an important factor in implementing the system, where BSSN can coordinate with the Ministry of Administrative and Bureaucratic of the Republic of Indonesia and the Ministry of Communications and Information Technology Indonesia.

4. Identity of Things.
   Standards are a challenge for host identification/system user authentication. At this stage, BSSN must accelerate the completion of regulatory preparation, which is still being hampered.

5. Logging.
   The event logging mechanism also poses a challenge to system security because, in the future, many systems will be implemented by central agencies and local governments. Once again, qualified system security personnel are required to log events. Therefore, BSSN, through the Deputy for Personnel Control Number 4, should coordinate with the Ministry of Administrative and Bureaucratic of the Republic of Indonesia to build qualified human resources in system security.

5. CONCLUSION AND RECOMMENDATION

The COVID-19 pandemic has given momentum to cyber criminals to launch attacks and cybercrimes. From January to April 2020, BSSN's National Cyber Security Operations Center recorded no less than 88 million cyber attacks in Indonesia. This number is fantastic and indicates the country's weakness in cyber defense.

Cyber attacks during this period were dominated by Trojans, which reached 56%, followed by information gathering at 43%. The rest were web application attacks. In addition, 25 cyber-attacks specifically utilized the COVID-19 issue, targeting global and Indonesian targets. Attacks with this mode vary from phishing e-mails and malware to spyware. Not only that, hundreds of website defacement cases also occurred during this period, generally targeting government websites.

The Tokopedia data leak incident involving millions of user data also occurred during the initial coronavirus outbreak in Indonesia. This further emphasizes that cybersecurity and personal data protection still need to be improved in Indonesia. Therefore, BSSN, as the leading sector of national cyber security, must develop an adequate and effective cyber defense strategy immediately.

In formulating the strategy, BSSN needs to pay attention to three important things: ends or goals, means or resources, and ways or methods/concepts. The ends in question are creating adequate cybersecurity and data protection for government systems and data and citizens' data. Resources include funds, advanced technology, and competent human resources in IT security. Methods or concepts concern the latest cyber defense methods and techniques applied.

In strategic management, three stages must be considered: strategy formulation, implementation, and evaluation. All three have a crucial role in ensuring that the cybersecurity strategy designed can run effectively and sustainably. With all three, the results achieved will be maximized.

With a well-thought-out cyber defense strategy and consistent implementation by BSSN and its partners, Indonesia's cyber security level is expected to increase significantly. Cyber threats are expected to continue to increase along with the development of technology and the digitalization of people's lives. So, preventive efforts and careful defense preparations from BSSN and all related parties are needed to protect government systems and data and the privacy of Indonesian citizens in cyberspace.

BSSN's role in securing the system certainly has its challenges that need to be anticipated, including challenges in maintaining data availability to remain high in the face of attacks, maintaining the confidentiality of personal data of system users, periodically repairing security holes (patching) in all system applications that continue to grow in number, authenticating system users amid the lack of digital identity standards (identity of things), and recording event logs (logging) on all systems in central and regional government agencies. To overcome these challenges, BSSN must coordinate and cooperate with relevant ministries such as the Ministry of Communications and Information Technology Indonesia. Regarding data centers and data interoperability, the Ministry of Administrative and Bureaucratic of the Republic of Indonesia regarding IT security human resource development and accelerating the preparation of relevant regulations to support BSSN's system security efforts. With proper anticipation through inter-agency coordination and regulatory support, BSSN is expected to be able to overcome challenges in its role of securing government electronic systems.

REFERENCES

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1). http://dx.doi.org/10.22212/jp.v5i1.336

B. S. dan S. N. (BSSN) and I. H. P. (IHP), (2019). "Laporan Tahunan Honeynet Project BSSN IHP 2019".

B. S. dan S. N. (BSSN) and I. H. P. (IHP), (2020). "Laporan Tahunan Honeynet Project BSSN IHP 2020".

BSSN. (2020). Rekap Serangan Siber (Januari - April 2020) Badan Siber dan Sandi Nasional : https://www.bssn.go.id/rekap-serangan-siber-januari-april-2020/

Buzan, B., & Hansen, L. (2007). *International Security*. London: SAGE Publication Ltd.

Center for Strategic & International Studies. 2020. Significant Cyber Incidents Since 2006. Washington D. C.: Center for Strategic & International Studies. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Creswell, John W. (2010). Research Design: Qualitative, Quantitative, and Mixed Approaches. Yogyakarta: Student Library.

Croft, S. (2006). Images and Imagining of security. UK: Warwick University. Melalui https://journals.sagepub.com/doi/abs/10.1177/0047117806069399 tanggal 10 april 2023 22.06 WIB

David, Fred R. (2011). Strategic Management: Concepts and Cases. New Jersey: Prentice Hall.

Ismansyah, I., Afrizal, R., & Arrahman, Z. (2023, July). Strategic policy in law enforcement against cybercrime during the COVID-19 pandemic in Indonesia. In *AIP Conference Proceedings* (Vol. 2722, No. 1). AIP Publishing.

Lukasik, S. J., Goodman, S. E. & Longhurst, D. W. (2003). Protecting Critical Infrastructures Against Cyber-Attack. New York: Oxford University Press Inc, p. 11

Lykke Jr, Arthur F. (1998). Military Strategy: Theory and Application. Pennsylvania: U.S. Army War College.

Rahmawati, C. (2020, November). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. In Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO) (Vol. 2, pp. 299-306).

Sims, Jonathan W. 2011. "Cyber Security: The Next Threat to National Security" United States Marine Corps Command and Staff College Marine Corps University.

Stevens, T. (2016). Cyber security and the politics of time. Cambridge University Press.

Suyanto, M. (2003). *Strategi periklanan pada e-commerce perusahaan top dunia*. Penerbit Andi.

Tambunan, B., Sihombing, H., Doloksaribu, A., & Muda, I. (2018, September). The effect of security transactions, ease of use, and the risk perception of interest in online buying on the e-commerce tokopedia site (Study on Tokopedia. id site users in Medan city). In *IOP Conference Series: Materials Science and Engineering* (Vol. 420, No. 1, p. 012118). IOP Publishing. https://doi.org/10.1088/1757-899X/420/1/012118

Triwahyuni, D. (2022). Indonesia Digital Economic Diplomacy during the Covid-19 Global Pandemic. *Journal of Eastern European and Central Asian Research (JEECAR)*, *9*(1), 75-83. https://doi.org/10.15549/jeecar.v9i1.880

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, *6*(1), 2319-2327.