The Ambassador Publishing
Quarterly Journal of Social and Political Sciences
Vol. 1 No.1 March 2024: 19-22
DOI: 10.62529/qjsps.v1i1.18
Open Access
Article Type: Policy Brief

Strategic Efforts in Encountering the Cyber Threats in the Time of Covid-19 Pandemic

Luthfania Andriani

BA in International Relations, Department of International Relations,
Faculty of Social and Political Sciences, Hasanuddin University, Makassar, Indonesia

Correspondence: Luthfania Andriani. E-mail: luthfania.andriani@gmail.com

RECEIVED 17 February 2024; **ACCEPTED** 27 February 2024; **PUBLISHED** 31 March 2024

Abstract: *The Covid-19 pandemic which has been a global health crisis not only posing threats in social, political, and economic sector, but also rising a big threat towards cybercrime. The state's priority tends to focus in controlling and addressing the pandemic is reducing controlling and surveillance priorities in the other sectors. This lead to the increasing gap of cybercrime to take place by leveraging the situation. Therefore, this policy brief will explain three outlines of policy options that could be taken by the Indonesia's National Cyber and Code Agency (NCCA) as efforts to optimize the cyber defense and security in facing the cybercrime in the Covid-19 pandemic, which are: 1) Strengthening the cyber defense of Indonesia which is extended to the company and online platform levels; 2) Enhanced cooperation in terms of sharing data in the regional level of ASEAN; and 3) Enhanced the engagement in terms of training, transfer of skill and knowledge in the international level. This policy brief then will recommends a policy to Indonesia's NCCA that could be applied optimally and effectively so that cyber threats in the time of Covid-19 pandemic could be reduced well with a maximum controlling.*

Keywords: *Covid-19 pandemic, cybercrime, cyber threats,*

1. Introduction

The implementation of the social and physical restrictions has led to almost every activities are shifted to indoor activities with less going outdoor. This requires the school and work activities to be done from home by using online facilities, such as through video conference applications or software, social media, websites, e-mails, etc. It gives chances for cybercrime to increase with the rising and massive internet and online users from various ages. Children, parents, or laymen exposed to cybercrime, there has to be involved and getting into internet activities. These people becomes susceptible to be attacked by the cybercrime because their lack of knowledge about cybercrime. The cybercrime actions then will likely be enhanced by the reduced of cyber surveillance and controlling resulting from social and physical restriction which reducing the outdoor activity and turning many sectors to be focus in controlling the pandemic. According to the NCCA data, during January to April 2020 period, there were approximately 88.414.296 cyber attacks with their peak attacks was reached in March, when the pandemic of Covid-19 just arose in Indoensia, with more than 29 thousands cyber attacks (BSSN, 2020, p. 11). Some of the attacks were conducted with a motive which are related to the pandemic. Pandemic leaves restless and worried societies are about vulnerable to be the target of the cyber attacks. The forms of cyber attacks are varying, such as e-mail phishing in the name of credible institution, like WHO, about pandemic information which contains a malware (UNODC, 2020, p. 2), message phishing or smishing which contains malware, telephone fraud through call center (Tidey, 2020), malware attack to the important institutions like hospital for the purpose of data theft (INTERPOL, 2020) that can result in a disruption of hospital operations, online fraud linked to the sales of medical supplies, such as masks (Europol, 2020), etc.

The implementation of social and physical restriction also complicate the access of transnational crime (TOC) which lead to many of TOC groups are using cybercrime as their alternative in getting profit as their source of funding. For example, a drug cartel which also doing malware attack besides to get profit for its members, but also to finance the drugs productions and distributions (UNODC, 2020, p. 25). The cybercrime group which also derived from other TOC groups in this pandemic time could increase the threats of TOC, especially after the pandemic as their funding still remained running smoothly through cybercrime actions. Within the pandemic period, the cybercrime also increases with many TOC groups which not normally doing cybercrime also committed in cybercrime.

The social and physical restrictions should not loosen or minimize the surveillance and controlling of cybercrime. Slow controlling could lead to a rise of cyber attacks which threatens individual in Indonesia because of the internet-oriented activities of the societies. The worst could result in the leak of state's data and secrets if the attacks have reached the states and official institutions. This could affect the later prospects the existence and sovereignty of Indonesia toward others.

2. Policy Options

2.1. Strengthening the cyber defense of Indonesia which is extended to the company and online platform levels

This policy is one of the earliest option that could be done by NCCA as an institution which is responsible to strengthening the cyber defense and surveillance in Indonesia. Strengthening the cyber defense system is extended to the company levels, both the private and official companies, and online platform levels which are vulnerable to be attacked in this pandemic time. Strengthening in cyber defense is carried out not only by updating the system gradually, but also doing early detection towards potential malware that potentially could be a cyber threat, and strengthening the internal institution of NCCA through mitigation efforts and control simulation if a cyber attack is happening. **Advantages:** Strengthening cyber defense in the company levels could minimalize the risk of high cost and loss to any company that could come later under the influence of cyber attacks. BSA estimates that less alertness of cyber defense in the company level will cost up to $750 billion during 2017 – 2025 (Bussiness Software Alliance, 2020, p. 8). This effort also could maintains the stability of companies' performance and profit to a minimum risk of high loss. Strengthening cyber defense in the online platform levels could make it easier to strengthen the users' security and address cybercrime for vulnerable societies. The NCCA's internal defense by mitigation measures could reduce the cost of later attacks by up to $680,000 (Bussiness Alliance Software, 2020, p. 5). Strengthening cyber defense in health companies could minimalize chaos and operational disruptions that could impede the treatment of Covid-19, such as those hospitals whose are vulnerable to be attacked by the cybercrime. This policy option is encouraging the self-sufficiency of Indonesia in developing cyber defense by maximizing the management of applications, cloud, and data centralization. **Disadvantages:** Strengthening cyber defense will take a long time in reaching the whole implementation, especially in mapping the strategic companies and online platform which would be enhanced for its cyber defense system. It refers to the implementation of this policy that could not be done directly in all companies and online platforms at once, so it must be phase out at some level of priority and risk for each company and platform. Long and gradual time of implementation could still be a gap of cybercrime to increase in some companies and platforms which are not strengthened yet.

2.2. Engagement in terms of sharing data in the regional level of ASEAN

This policy is committed to make a good use of regional institution of ASEAN, which provides collaboration within ASEAN countries in addressing regional issues. The threat of cybercrime is not only a threat for Indonesia, but also for the regional of ASEAN. Therefore, it is an opportunity to build cooperation within ASEAN countries in controlling the cybercrime, especially in organizing data sharing and data centralization. This cooperation is undertaken by states to share information each other about cyber attacks that have been detected and potentially be a threat for others. In the consequences, those potential cyber attacks could be preventable before it getting increased. **Advantages:** Effort at this ASEAN level of cooperation could ease the ASEAN countries to minimize the risk of high costs because the lack of cyber defense. AT Kerney estimates that ASEAN countries with its current ability of cyber defense could

cost up to $171 billion for cyber defense by 2025 (Thomas, 2019). As the closest and most strategic institution for Indonesia, ASEAN is one of the truthful cooperation to be engaged with. It has minimum risk of losing data rather than cooperation in international level. This refers to ASEAN as a region which is formed based on strong sense of belonging, so ASEAN countries are strongly embedded together (Geotimes, 2019). Data centralization could ease the data control and management, especially when there is a problem or a threat of attack on the data. **Disadvantages:** ASEAN is a region of countries with inadequate capability of cyber defense. It tends to take a long time to provide a maximum and efficient data sharing cooperation. This is because of ASEAN was not fully targeted for cybercrime before, so reinforcement of cyber defense was not being a high and fully priority until the threats of cybercrime in ASEAN are emerged (Bussiness Software Alliance, 2020, p. 8). Cooperation at ASEAN level will require high costs of funding to build or provide advanced technologies which cost highly for ASEAN countries itself. According to the current financing of each ASEAN countries in cyber defense, it costs about 0,06% of ASEAN's GDP while it requires 6 times more (0.61% of ASEAN's GDP) in developing adequate cyber defense (Thomas, 2019). Data centralization is at a high risk if they are exposed to a cyber attack that could threaten the overall data to be lost, stolen, and abused.

2.3. Enhanced the engagement in terms of training, transfer of skill and knowledge in the international level

This policy is one of the options that could be done with Indonesia's engagement in international level of cooperation. The cybercrime that poses a threat not only to Indonesia, but it has threatened global security. This encourage a potential cooperation to be committed by countries in reinforcing the capability of theirs cyber defense. Cooperation through training and transfer technology and knowledge is made to help each other in strengthening each countries' capability to understand about the cyber crime and how to address and be aware of it. **Advantages:** Cooperation at the international level could make co-operating partner more strategic to fit with Indonesia's need and ability for reinforcing the capabilities from countries whose have advanced capabilities of cyber defense already. It is also a good opportunity to enhance Indonesia's partnership and interdependence with other countries. **Disadvantages:** Involving countries which are not embedded strongly like in a region level could be a gap for political strategy in resulting high risk for Indonesia. By leveraging the pandemic situation, political strategy of the advanced countries towards developing countries could be increased in exploiting the developing countries (Crisis Group, 2020). Therefore, it is vulnerable as a threat towards Indonesia's sovereignty if Indonesia is not carefully choosing the strategic co-operating partners. However, building cooperation with countries which are not strongly embedded will take a long time because it takes time to build a same vision and mission towards the cooperation.

3. Conclusion and Policy Recommendation

The increasing risk of high threats of cybercrime in the Covid-19 pandemic time requires prompt and suitable measures from the NCCA to minimalize the potential threats. Therefore, those three policy options above could be committed with prioritizing in the strengthening the cyber defense of Indonesia which is extended to the company and online platform levels. It is because the potential threat of cybercrime highly comes from the users itself which are rising highly in the pandemic time, so NCCA's internal reinforcement is required. While, cooperation in regional and international level is likely difficult to be carried out in the pandemic time as each country tends to focus in addressing its domestic conditions as the impact of pandemic. Consequently, independent efforts of Indonesia in strengthening the cyber defense through NCCA should be crucial. It is also highly important to emphasize the role of NCCA as the main supportive institution for Indonesia's cyber defense when other sectors are largely mobilized in addressing the Covid-19 pandemic.

References

Badan Siber dan Sandi Negara. 2020. "Buku Putih Keamanan Siber Sektor Kesehatan". Direktorat Proteksi Infrastruktur Informasi Kritikal Nasional. Depok. <https://cloud.bssn.go.id/s/4DxxKp3eeeyb6Xb#pdfviewer>

Badan Siber dan Sandi Negara. 20 April. 2020. “Rekap Serangan Siber (Januari – April 2020)”. Diakses pada tanggal 24 Mei 2020. <https://bssn.go.id/rekap-serangan-siber-januari-april-2020/>

Badan Siber dan Sandi Negara. 20 April 2020. “Rekapitulasi Insiden WEB Defacement Periode Januari 2020 – April 2020”. Pusat Operasi Keamanan Siber Nasional BSSN. Depok. <https://cloud.bssn.go.id/s/qpBD4mbZCmL3F85>

Badan Siber dan Sandi Negara. 19 Mei 2020. “Melalui Kolaborasi Seluruh Pemangku Kepentingan Keamanan Siber, Indonesia Mampu Hadapi Tantangan dan Ancaman Siber dalam Tatanan Hidup Normal Baru di Tengah Pandemi Covid-19”. Diakses pada tanggal 24 Mei 2020. <https://bssn.go.id/melalui-kolaborasi-seluruh-pemangku-kepentingan-keamanan-siber-indonesia-mampu-hadapi-tantangan-dan-ancaman-siber-dalam-tatanan-hidup-normal-baru-di-tengah-pandemi-covid-19>

Business Software Alliance. 5 Mei 2020. “COVID-19 dan Ancaman Siber di Asia Tenggara”. The Software Alliance. Singapura. <https://cyberfraudprevention-bsa.com>

Crisis Group. 20 Maret 2020. “ Covid-19 and Conflict: Seven Trends to Watch”. Diakses pada tanggal 19 Mei 2020. <https://crisisgroup.org/global/sb4-covid-19-and-conflict-seven-trends-watch>

Europol. 27 Maret 2020. “How Criminals Profit From The Covid-19 Pandemic”. Diakses pada tanggal 18 Mei 2020. https://europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic

Ghifari, Razan. 22 September 2019. “Ada Apa dengan Hubungan Indonesia dan Asia Tenggara?”. Diakses pada tanggal 24 Mei 2020. <https://geotimes.co.id/ep-ed/ada-apa-dengan-hubungan-indonesia-dan-asia-tenggara>

INTERPOL. 13 Maret 2020. “INTERPOL Warns of Financial Fraud Linked to Covid-19”. Diakses pada tanggal 19 Mei 2020. <https://interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-covid-19>

Kumar, Isabelle dan Alice Tidey. 30 Maret 2020. “Covid-19: Organised Crime Group Adapting with New Crime Trends, Interpol Warns”. Diakses pada tanggal 18 Mei 2020. <https://www.euronews.com/amp/2020/03/30/covid-19-organised-crime-group-adapting-with-new-crime-trends-interpol-warns>

Nainggolan, Oki Rilo. Oktober 2017. “Kepentingan Indonesia Bekerjasama dengan Jepang dalam Bidang Pertahanan Tahun 2015”. JOM FISIP. Vol. 4 No. 2. https://medianeliti.com/media/publications/205888-kepentingan-indonesia-bekerjasama-dengan-jepang-dalam-bidang-pertahanan-tahun-2015

Thomas, Jason. 3 Agustus 2019. “Intensifying ASEAN’s Cybersecurity Efforts”. Diakses pada tanggal 24 Mei 2020. <https://theaseanpost.com/article/intensifying-aseans-cybersecurity-efforts>

Thomas, Jason. 10 September 2019. “Ransomware Could Cripple ASEAN”. Diakses pada tanggal 24 Mei 2020. <https://theaseanpost.com/article/ransomware-could-cripple-asean>

United Nations Office on Drugs and Crime. 14 April 2020. “Cybercrime and COVID-19: Risks and Responses”. United Nations Office on Drugs and Crime. Vienna. <https://undoc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf>

United Nations Office on Drugs and Crime Research and Trend Analysis Branch. Mei 2020. “COVID-19 and the Drug Supply Chain: From Production and Trafficking to Use”. United Nations Office on Drugs and Crime. Vienna. <https://www.unodc.org/documents/data-and-analysis/covid-Covid-19-and-drug-supply-chain-Mai2020.pdf&ved=2ahUKEwjfh-K79s7pAhWRfn0KHe-eDEQFjAAegQIAhAB&usg=A0vVaw2bm50SHgChuCimsf71v5zI>