NDCP Executive Policy Brief

A PUBLICATION SERIES ON NATIONAL SECURITY ISSUES
BY THE NATIONAL DEFENSE COLLEGE OF THE PHILIPPINES

26 March 2021
No. 2021-02

Pursuing Regional Cyber Cooperation: Implications for the Philippines and the ASEAN

Christine Lisette M Castillo

Introduction

Cyberspace is a global domain that brings states and people together. It is considered as one of the global commons alongside the high seas, airspace, and outer space, which all states have legal access.[1] Cyberspace is used not only by technical experts but by all institutions and individuals around the world. Due to the domain's interconnected nature, state borders become irrelevant as threats in cyberspace can disrupt the international system at once. In this regard, a collective response is necessary in addition to the individual efforts that governments pursue.

The Philippines, as a founding member of the Association of Southeast Asian Nations (ASEAN), must contribute towards fostering a strong collective cyberspace cooperation in the regional setting. Given that the Philippine cyberspace is prone to attacks that have political, economic, and socio-cultural repercussions, active participation in cybersecurity cooperation agreements while developing its cyber defense and capabilities is an opportunity that the country must explore.

This policy brief aims to discuss how cyber cooperation can be advanced in the region. In particular, it seeks to answer the following questions: 1) How important is cyber cooperation in Southeast Asia?; 2) What are the challenges of regional cyber cooperation in the ASEAN?; and 3) How can the Philippines effectively contribute to regional cyber cooperation? This policy brief argues that ASEAN is instrumental in leading regional cyber cooperation and that the Philippines must address its cyber challenges in realization of its role.[2]

Cyber Cooperation in Southeast Asia: Opportunities and Challenges

The Southeast Asian region deals with opportunities and challenges in cyberspace. This situation creates an environment where securing cyberspace cannot be accomplished in isolation and in reliance to the initiatives done individually by states, but rather through a collective response that bears more magnitude. It is thus important to strengthen cyber cooperation in the region not just through government channels but also through the involvement of private actors because of several reasons:

First: growing number of netizens.[3] The region had 40 million new Internet users in 2020 alone, compared to the 100 million between 2015 and 2019.[4] This makes 70% of the regional population online. The acceleration of digital consumption was brought by the need to use new digital services due to the COVID-19 pandemic,[5] such as the Internet for daily news and Digital Financial Services (DFS) for online transactions.[6] In addition, 8 out of 10 believed that technology was useful during the pandemic in areas such as providing access to basic and essential services, education, and professional work.[7] Indeed, technology's impact has fundamentally increased in all areas of life for the past year. In turn, these developments make Southeast Asia a prime target for cyber criminals to exploit a larger market, gaining more prospects to conduct illicit activities such as phishing, cyber scams, and e-commerce data interception, which the ASEAN Cyberthreat Assessment 2021 of the INTERPOL identified as some of the region's top cyberthreats in 2020.[8] As this is likely to be sustained even after the pandemic, the protection of netizens in the region must be ensured.

Second: regional stability. Cyber cooperation has economic and security implications. One of the goals of the ASEAN is regional economic integration which can be achieved through the ASEAN Economic Community (AEC) Blueprint 2025. In this framework, the ASEAN recognizes the need to embrace evolving digital technology as means "to enhance trade and investments, provide an e-based business platform,

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

promote good governance, and facilitate the use of green technology."[9] Indeed, a sustainable, resilient, and competitive economy requires an attention to cyber cooperation. This will guarantee an inclusive, transformative, and secure cyberspace where no country is left behind.[10] In terms of security, the cyber threats posed by the great power competition in the region between the United States and China can continue to change the regional security landscape with detriment. Hence, cyber cooperation will provide the region a united front amid this dynamic. As these two countries are cyber powers themselves, cyber cooperation will also encourage a more responsible use of cyberspace and inhibit any act of cyber espionage orchestrated by both for their respective security and economic gains.[11]

Third: pool of cybersecurity experts. The shortage of skilled cybersecurity professionals in the region, particularly in Vietnam, Indonesia, Malaysia, and the Philippines, is alarming because these experts are the driving force of cybersecurity.[12] A few seconds without proper monitoring and managing of the cyber domain can create lasting damages. In this regard, cyber cooperation is a tool for the development and training of cybersecurity experts among the ASEAN member states which is a vital step towards thwarting cyber attacks and advancing the cyber capability of the entire region. It is also important to highlight the crucial role of the ASEAN youth for the future of cybersecurity. Cyber cooperation can be done through providing scholarship programs and incorporating the cyber component in schools' curricula. Also, interactive workshops and camps can be an avenue for the ASEAN youth to convene and have a first-hand experience in addressing the region's cyber challenges.[13] Greater connectivity means higher probabilities of cross-border cyber threats.[14] Now more than ever, the pool of cybersecurity experts must increase.

The advantages of cyber cooperation are constrained by the following points of consideration:

First, the uncertain nature of cyberspace generates hesitation for cyber cooperation as states are too careful to trust others, most especially if cooperation involves a state that is known to launch covert cyber operations and cyber attacks. To note, trust and confidence must be built before cooperation takes place.[15]

Second, there exists a digital divide among the ASEAN member states as explained by the varying levels of cyber capabilities and information and communications technology (ICT) development.[16] With this, it has been difficult to actively exercise cyber cooperation and efforts to implement regional frameworks have been faced with challenges.

Third, governments are currently focused in addressing the COVID-19 pandemic, which takes up most of the resources and discussion agenda of bilateral and multilateral engagements among countries, specifically in Southeast Asia.

The regional community must find a way to overcome these challenges and effectively come together to achieve cybersecurity. To this end, the initiatives of the ASEAN are significant.

The Role of the ASEAN in Regional Cyber Cooperation

Cyberspace is a novel area of discussion compared to other issues that are often discussed in the regional setting. This is because cyber issues can be initially viewed merely as a national topic within states rather than among them. On the contrary, cyberspace is a collaborative issue that requires a cohesive cyber cooperation among the ASEAN member states.[17] The ASEAN has pursued the following initiatives:

ASEAN ICT Masterplan 2020 (AIM 2020). On November 2015, AIM 2020 was approved by the 15th ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN) (ASEAN Digital Ministers Meeting (ADGMIN) at present) in Vietnam to highlight the central role of information and communications technology to the economic and social development of the region. The masterplan covers the period from 2016 to 2020 and security is outlined among its six-point vision, as the masterplan aims to achieve "a safe and trusted ICT environment in ASEAN."[18] Because of the progress that AIM 2020 accomplished, several frameworks that will serve as basis for the next masterplan have been approved, one of which is the ASEAN Cybersecurity Cooperation Strategy that will focus on strengthening cooperation in cybersecurity incident response, Computer Emergency Response Team (CERT), and cybersecurity capacity building.[19]

Master Plan on ASEAN Connectivity 2025. The ASEAN member states have formulated the Master Plan on ASEAN Connectivity 2025, which highlights digital innovation as one of the strategic areas to achieve the vision of a connected and integrated ASEAN.[20] Meanwhile, in a similar document, the ASEAN Digital Masterplan 2025, one of the intended outcomes is a secure and trusted digital environment

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

"where transactions and information exchanges are safe, secure, and trustworthy."[21] Indeed, the trust of consumers is important if digital services ought to be adopted.[22] Also notable in this masterplan is the promotion of developing digital skills such as coding and programming which can be offered in training courses and bootcamps through the collaborative effort of the ASEAN member states.[23]

ADMM Plus Experts Working Group (EWG) on Cybersecurity. With the proposal of the Philippines to establish a cybersecurity working group under the ambit of the ASEAN Defense Ministers Meeting Plus (ADMM-Plus),[24] the defense chiefs of ADMM-Plus adopted the creation of a working group that aimed to enhance the capability of the region to secure its cyberspace and promote "practical and effective cooperation".[25] Under the EWG, cooperation may range from meetings on sharing information and experiences on cyber issues to the conduct of trainings and exercises and sharing of appropriate technologies, equipment, and resources to address cyber challenges as one regional community.[26] On 1-2 August 2019, the Philippines and New Zealand hosted a Table-Top Exercise (TTX) to challenge the EWG on assessment, analysis, and resolution of complex cyber threats.[27]

Computer Emergency Response Team (CERT).[28] Every year, the ASEAN CERT Incident Drills (ACID) is held to strengthen the cybersecurity preparedness of the region in terms of incident response procedures. ACID is designed with different scenarios and different levels of complexity which aims to develop trust among the CERTs of the ASEAN members states and its dialogue partners.[29] In relation, the Asia Pacific Computer Emergency Response Team (APCERT), to which the ASEAN member states are a part of, facilitates cooperation and information-sharing, and promotes research and development.[30] APCERT aims to strengthen Asia-Pacific's "collective ability to detect, prevent and mitigate" malicious cyber activities through collaborative action points such as joint development of measures for large-scale or regional network security incidents and information sharing and technology exchange on cybersecurity.[31]

Norms. The ASEAN member states have agreed amongst themselves to enhance cooperation towards building "an open, secure, stable, accessible, and resilient cyberspace".[32] The ASEAN also planned to adopt "a set of common, voluntary, and non-binding norms of responsible state behavior in cyberspace."[33] Through the ASEAN Ministerial Conference on Cybersecurity (AMCC), Singapore was tasked to lead the enhancement of cyber coordination in the region. The central theme of this task is the creation of voluntary norms for state behavior in cyberspace, anchored on the 11 norms[34] stated in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of UNGGE (UNGGE 2015). Even though the UNGGE 2015 was stalled two years later and there has been no clear direction for implementation, the ASEAN continues to pursue its initiatives on the establishment of norms for cybersecurity.[35]

External linkages. Externally, the ASEAN has partnered with the European Union (EU), the World Economic Forum (WEF), and the United States (US) on cybersecurity cooperation. For one, the ASEAN-EU Statement on Cybersecurity Cooperation, adopted in 2019, laid down points of commitment and convergence and took note of the role that inter-state cooperation and multilateral discussions have on cybersecurity in the region.[36] Meanwhile, the Statement on Cybersecurity Cooperation with the US recognized the pervasiveness of cyber threats and reaffirmed the commitment to work together and bridge ICT development gaps with the ASEAN.[37] Finally, the cooperation between the ASEAN and the WEF focuses on the ASEAN as the "fastest growing Internet market in the world", to which the cooperation aims to contribute to a "sustainable, inclusive, and trustworthy" digital ecosystem in a complex and changing region.[38]

Although the vision is set and the aforementioned initiatives are present, cyber cooperation remains to be a lesser priority for states as the productive progress on it for the past year has been slow. In this context, the ASEAN member states must rethink their priorities and continue to cooperate on cybersecurity as cyber threats also continue to proliferate in any situation. This especially applies to the Philippines in particular, which is a common target of cyber threat actors.

Cybersecurity Considerations for the Philippines

The Philippines is an active participant in ASEAN-related activities and initiatives. Aside from what was mentioned in the previous section, the country has also established cooperation with countries that share the same commitment such as Australia and Japan, with activities covering cyber capability enhancement, skills training, and cyber defense. In spite of these, the Philippines might take on a peripheral role in regional cyber cooperation because of two key issues.

First. It can be noted that the Philippines'

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

National Cybersecurity Plan (NCSP) 2022 sets the government strategy on cyberspace. Although the plan discussed the regional cyber threat landscape, there is no extensive cyber cooperation strategy except for a brief section on the importance of international collaboration.[39] Hence, the plan focuses more on domestic cyber capability enhancement without definitive courses of action on how to proceed with establishing or developing cyber cooperation with its regional neighbors. This is not to suggest that the Philippines should not focus on building its domestic cyber capability. To the contrary, strengthening the country's internal capacity must be the first step towards combating cyber threats. Rather, this is to underscore that cooperation is imperative in addressing security threats in cyberspace. Although the Philippines and China co-chaired the first ASEAN-China Cyber Dialogue on December 2020,[40] which is an important step towards greater collaboration in the region and in establishing the Philippines' commitment for the protection of the regional cyberspace, the absence of a cyber cooperation strategy in the Philippines' prime cybersecurity plan remains to be a vital concern.

Second. Data in 2016 revealed that the Philippines only has 84 Certified Information Security Systems Professionals (CISSP), a very insufficient number in relation to the increasing sophisticated data breaches that both public and private institutions in the country experience.[41] This makes the country's IT capabilities relatively weak in comparison with the rest of the ASEAN.[42] This challenge can be traced to the low level of public awareness of cyber issues as well as the dearth of opportunities for students to pursue a career in cybersecurity. Only three (3) universities in the country offer a cybersecurity-related program: AMA University, with its Bachelor of Science in Cybersecurity;[43] Holy Angel University, with its Professional Science Master's in Cybersecurity;[44] and Ateneo de Davao University, with its inclusion of a Cybersecurity Track under the Bachelor of Science in Information Technology program.[45] In addition, there has not been a significant update on the Php 300 million Cyber Training Facility to which the process of implementation started in 2019.[46]

Policy Recommendations

With cyber criminals and threat actors constantly adapting to developments in cyberspace, the ASEAN member states must harness their collective power and strive to be multiple steps ahead in order to prepare, prevent, respond, and resolve cyber challenges in the region. The following policy recommendations are presented:

Create a cybersecurity cooperation plan. This policy recommendation is directed to the Philippines. As discussed in the preceding section, the NCSP 2022 document lacks clear mechanisms on cross-country collaboration, which should be essential in consideration of the cyber situation at present. The creation of a cybersecurity cooperation plan can be done in two ways: first, for the NCSP 2022 to have a supplemental section on international and regional cybersecurity cooperation; and second, to create a separate document that discusses the strategy extensively. Either way, the plan must contain the key issues that the Philippines wants to pursue in establishing cooperation with others, the key components of the cooperation, and what the parties in the cooperation hope to achieve as the result. The plan must not be limited to the ASEAN but include collaboration with like-minded states and institutions across the globe.

Review Master Plan on ASEAN Connectivity 2025. The strategic area on digital innovation must not only focus on an inclusive digital development to bridge the digital divide but also on a secure and resilient regional cyberspace to protect the data and information of all stakeholders. The Department of Information and Communications Technonology (DICT), together with the Department of Foreign Affairs (DFA) can coordinate with their counterparts in other ASEAN member states in this regard.

Finalize the establishment of cyber norms. For the past years, there have been proposals and discussions on the establishment of norms that will lead to the responsible use and exploration of regional cyberspace. Through the ASEAN Ministerial Meeting on Cybersecurity, member states have expressed support to adopt basic, operational, and voluntary norms to guide the use of ICT in the region. However, regional norms in cyberspace are still subject to contestation. Hence, the discussions on cyber norms are yet to be translated to actual results.[47] The Philippines can promote and encourage the development of cyber norms as its success will provide a more robust protection against cyber hacking, cyber espionage, and other cyber threats that the country experiences. Once finalized, the Philippines shall follow and adhere to the cyber norms.

Promote confidence-building measures. To foster an effective collaboration, the ASEAN member states must first build confidence and trust with one another. This can be done through bilateral, multilateral, or even minilateral engagements not only

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

among government institutions but also among non-government institutions and representative individuals.

Continue cyber initiatives toward the shared goal. The ASEAN member states must not fixate on the digital divide in the region but rather on the common cyber issue that all member states experience. No member is exempt from cyber threats, even in consideration of its cyber capabilities. In ASEAN, one of the main rationale in pursuing cyber cooperation is the achievement of a secure cyberspace that will safeguard and ensure the economic growth of the region. This can be the motivation of member states to further their cooperation and become more active in regional cyber dialogues.

Conclusion

The interconnectedness of cyberspace and the challenges with it require a collective response that will provide advantages for the ASEAN member states. As a region which values economic growth but is threatened by cyber risks, Southeast Asia must view cyber cooperation as the key moving forward. However, the region is diverse in culture, politics, and economy. In a way, the differences affect the ASEAN member states' prioritization of national interests and in this case, cybersecurity. Further, there is a digital divide or varying levels of cyber capabilities that constraint the ease of cooperation. To address this, it is important to note that although ICT infrastructure falls under the jurisdiction of states, cyber domain remains unconfined.[48] It is urgent to discuss these differences as cyberspace remains to be strategically used by states and non-state actors to launch crippling cyber attacks towards adversaries without necessarily triggering a war. The challenge, therefore, is to synchronize each point of view and establish a unified cooperation that will result to a secure, resilient, and progressive regional cyberspace.[49]

In the Philippines, a concern that necessitates attention is the cybersecurity skills deficit as the number of cybersecurity professionals in the country is not enough to manage the presence of a sizable population in cyberspace. Without establishing a cybersecurity workforce, the country cannot effectively contribute to regional cybersecurity cooperation. The absence of a clear framework for cyber cooperation in the NCSP 2022 albeit participation in actual cybersecurity dialogues is also an important gap that needs to be addressed.

Henceforth, the ASEAN member states must calibrate their differences and move towards the similar vision on cybersecurity, and the Philippines must continue to develop its domestic cyber capabilities as part of the regional community. Above all, a secure cyberspace is a secure ASEAN.

# # #

Christine Lisette M. Castillo *is a Defense Research Officer II at the Research and Special Studies Division of the National Defense College of the Philippines (NDCP).* *The views expressed in this policy brief are those of the author alone and do not necessarily reflect the views of NDCP. The readers are free to reproduce copies or quote any part provided proper citations are made. For comments and suggestions, please email* *christinelisettecastillo@gmail.com.*

Endnotes

[1] Andre Barrinha and Thomas Renard, "Cyber-diplomacy: the making of an international society in the digital age," *Global Affairs* 3, nos. 4-5 (2017): 357. https://doi.org/10.1080/23340460.2017.1414924.

[2] This policy brief falls under the NDCP's research focus areas of: a) Inclusive Security, which explores how technological developments can alter prevailing security thinking; and b) International Security Cooperation, which highlights the importance of international engagements to pursue Philippine national interests and "maintain peace in the region."

[3] A netizen is an individual who uses the Internet or someone who's part of the online community.

[4] Google, Temasek,and Bain & Company, *e-Conomy SEA 2020* (2020), 12, https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf.

[5] Google, Temasek,and Bain & Company, 13.

[6] Google, Temasek,and Bain & Company, 9.

[7] Google, Temasek,and Bain & Company, 20.

[8] INTERPOL Global Complex for Innovation, *ASEAN Cyberthreat Assessment 2021* (Singapore: INTERPOL, 2021).

[9] Association of Southeast Asian Nations (ASEAN), *ASEAN Economic Community Blueprint 2025* (Jakarta: The ASEAN Secretariat, 2015), 1. https://www.asean.org/storage/2016/03/AECBP_2025r_FINAL.pdf.

[10] Association of Southeast Asian Nations (ASEAN), 23-24.

[11] Caitriona H. Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," *Asia Policy,* no. 18 (2014): 135. https://www.jstor.org/stable/10.2307/24905282.

[12] Australian Cyber Security Growth Network, *Cybersecurity Opportunities in the ASEAN Region* (Commonwealth of Australia, 2019).

[13] Caitriona H. Heinl, "Enhancing ASEAN-wide Cybersecurity: Time for a Hub of Excellence?," *RSIS Commentaries*, no. 133 (2013): 1-2. https://www.files.ethz.ch/isn/172058/RSIS1332013.pdf.

[14] Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," 137.

[15] Fauzia Gustarina Cempaka Timur, "The Rise of Cyber Diplomacy – ASEAN's Perspective in Cyber Security," *The International Conference on Design and Technology* 2017, (2016): 246. DOI 10.18502/kss.v2i4.893.

[16] Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," 141.

[17] Heinl, 134.

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

[18] ASEAN, *Final Review ASEAN ICT Masterplan 2020* (Jakarta: The ASEAN Secretariat, 2020) 8. https://asean.org/storage/V4.-Final-Draft-_-AIM2020_Review_FInal_Draft_19Nov2020.pdf.

[19] ASEAN, 42

[20] ASEAN, *Master Plan on ASEAN Connectivity 2025* (Jakarta: The ASEAN Secretariat, 2016), 9. https://asean.org/storage/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf.

[21] ASEAN, *ASEAN Digital Masterplan 2025* (Jakarta: The ASEAN Secretariat, 2021), 41. https://asean.org/storage/ASEAN-Digital-Masterplan-2025.pdf.

[22] ASEAN, 64.

[23] ASEAN, 112.

[24] The ADMM-Plus is composed of the 10 ASEAN member states plus dialogue partners Australia, China, India, Japan, New Zealand, Republic of Korea, Russia, and the United States.

[25] ASEAN Defense Ministers' Meeting, *Establishment of the ADMM-Plus Experts' Working Group on Cybersecurity Concept Paper* (2016), 1-3. https://admm.asean.org/dmdocuments/Concept%20Paper%20on%20Establishment%20of%20EWG%20on%20Cyber%20Security,%20Final,%20as%20adopted%20by%20the%2010th%20ADMM.pdf.

[26] Ibid.

[27] Department of National Defense, "ADMM-Plus conducts Table-Top Exercise on Cyber Security," August 3, 2019, https://www.dnd.gov.ph/Postings/Post/ADMM-Plus%20conducts%20Table-Top%20Exercise%20on%20Cyber%20Security/.

[28] A CERT is a group of cybersecurity experts who deals with incidents in cyberspace. They have the responsibility to anticipate, prepare, prevent, respond, and resolve any form of cyber threat and cyber attack.

[29] The dialogue partners are Australia, China, India, Japan, and South Korea.

Cyber Security Agency of Singapore, "15th iteration of ASEAN CERT Incident Drill tests CERTs' preparedness against opportunistic COVID-19-related campaigns," *CSA Singapore*, October 8, 2020, https://www.csa.gov.sg/news/news-articles/15th-asean-cert-incident-drill.

[30] Khanisa, "A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation," *Journal of ASEAN Studies* 1, no. 1 (2013): 47.

[31] APCERT Secretariat, *APCERT Annual Report 2019* (2020). http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf.

[32] Jessica Haworth, "ASEAN nations strengthen cybersecurity ties through new cooperation agreement," *The Daily Swig,* July 10, 2019, https://portswigger.net/daily-swig/asean-nations-strengthen-cybersecurity-ties-through-new-cooperation-agreement.

[33] Haworth, "ASEAN nations strengthen cybersecurity ties through new cooperation agreement."

[34] For the list of norms, see https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[35] Benjamin Ang, "Next Steps for Cyber Norms in ASEAN," *RSIS Commentary,* no. 174 (2018). https://www.rsis.edu.sg/rsis-publication/cens/next-steps-for-cyber-norms-in-asean/#.YFvuma8zbIU.

[36] ASEAN, "ASEAN-EU Statement on Cybersecurity Cooperation," August 1, 2019, https://asean.org/asean-eu-statement-cybersecurity-cooperation/.

[37] ASEAN, "ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, November 16, 2018, https://asean.org/asean-united-states-leaders-statement-cybersecurity-cooperation/.

[38] World Economic Forum, "Digital ASEAN," https://www.weforum.org/projects/digital-asean.

[39] Department of Information and Communications Technology. Cybercrime Investigation and Coordination Center. *National Cybersecurity Plan 2022.* 30.

[40] Department of Foreign Affairs, "PH, China co-chair First ASEAN-China Cyber Dialogue," December 9, 2020, https://dfa.gov.ph/dfa-news/dfa-releasesupdate/28350-ph-china-co-chair-first-asean-china-cyber-dialogue.

[41] No recent data was available. Ted P. Torres, "Lack of IT security professionals makes Philippines prone to cyber crime," *The Philippine Star*, April 11, 2016, https://www.philstar.com/business/banking/2016/04/11/1571843/lack-it-security-professionals-makes-philippines-prone-cyber-crime.

[42] Australian Cyber Security Growth Network, *Cybersecurity Opportunities in the ASEAN Region*, 30.

[43] AMA Education System News, "BS Cybersecurity Now Offered at AMA University, https://news.amaes.edu.ph/2018/10/bs-cybersecurity-now-offered-at-ama.html.

[44] Sun Star Pampanga, "HAU launches PSM in Cybersecurity," *Press Reader*, May 10, 2018, https://www.pressreader.com/philippines/sunstar-pampanga/20180510/281603831102640.

[45] Percival Cyber Vargas, "Cybersecurity offered as new BS-IT track," *Atenews*, October 18, 2019, https://atenews.ph/news/cybersecurity-offered-as-new-bs-it-track.

[46] Denise A. Valdez, "P300-M cybersecurity center going up for bid," *Business World,* June 3, 2019, https://www.bworldonline.com/%E2%82%B1300-m-cybersecurity-center-going-up-for-bid/.

[47] This policy recommendation is in relation to the author's Executive Policy Brief dated 26 June 2020. The policy brief can be accessed at http://www.ndcp.edu.ph/wp-content/uploads/publications/2020/EPB_2020-02_Castillo.pdf.

[48] Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," 141.

[49] Timur, "The Rise of Cyber Diplomacy – ASEAN's Perspective in Cyber Security," 246.

Published by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph