NDCP Executive Policy Brief

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

24 December 2020
No. 2020-07

Defending the Philippines' Cyberspace Amid COVID-19

Christine Lisette M Castillo

Introduction

On 30 January 2020, the World Health Organization (WHO) declared a global health emergency over the novel coronavirus outbreak that emerged from Wuhan City in Hubei Province, China.[1] Subsequently, the virus was officially named the Coronavirus Disease 2019 (COVID-19), a disease caused by a newly-identified severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).[2] Due to its severity and spread, COVID-19 was later characterized as a pandemic.[3] This sequence of events have alarmed governments around the world, most especially those with weaker health systems, to review and evaluate plans to combat infectious diseases.[4]

> ***"A strong cyber defense is necessary to prevent and detect cyber attacks, and provide timely response to safeguard health, military, and other vital systems."***

As governments were occupied in addressing the health consequences of the COVID-19 pandemic, attacks in cyberspace have proliferated.[5] The implementation of a work-from-home arrangement during the pandemic meant that more private information technology (IT) devices are being used for official business.[6] Also, as people are required to stay in their houses because of the lockdown, their reliance on cyberspace for work, chores, and banking heightened. The WHO reported a five-fold increase in cyber attacks directed to its staff since the pandemic started.[7] Likewise, the United States Federal Bureau of Investigation (FBI) said that there has been a spike in cybercrime reports, four times more compared to the months before the pandemic.[8] Cyber attacks were also rising in Southeast Asia.[9] According to the National Bureau of Investigation Cyber Crimes Division (NBI-CCD), phishing is considered as the top cyber crime in the Philippines during the pandemic, with cases rising over 200 percent.[10] These reports signal that a strong cyber defense is necessary to prevent and detect cyber attacks, and provide timely response to safeguard health, military, and other vital systems.

Indeed, the cyber threats brought by the pandemic towards private and public stakeholders present a national security issue that needs to be addressed. This policy brief aims to examine the cyber threat landscape amid the COVID-19 pandemic. In particular, it seeks to answer the following questions: a) What are the prevalent cyber threats during the COVID-19 pandemic?; b) How can cyber defense be improved to combat cyber threats?; and c) How can a post-COVID-19 Philippines be perceived in the context of cybersecurity? This policy brief argues that developing the Philippines' cyber defense capability will aid the country in addressing cyber threats amid the COVID-19 pandemic and beyond.

Cyber Threats During COVID-19

In the Philippines' National Security

Policy (NSP) 2017-2022, cybercrime is revealed as today's fastest rising economic crime, with more and more criminals using the speed, convenience, and anonymity that the Internet provides.[11] With this, the government's 12-point national security agenda identified the importance of the informational and cybersecurity goal, which aims to safeguard classified and sensitive government records including state secrets from espionage and to shield the country from cyber attacks that can affect both private and public critical infrastructures.[12] In relation, the National Security Strategy (NSS), which was published a year after, noted cybersecurity as a core national interest i.e. "Protection of the Filipino public from criminality, illegal drugs, pandemics, cyber-attack, and weapons of mass destruction."[13] Ultimately, to provide a strong cyber infrastructure and cybersecurity is one of the goals of the NSS.[14] These pronouncements, albeit important, require action and commitment to effectively combat cyber threats during the pandemic.

It was established that the pandemic has not only disrupted the physical domain but also cyberspace. However, contrary to popular assumptions, the prevalence of cyber attacks during a pandemic is not new. The Ebola pandemic in 2014 was also plagued with cyber issues, specifically phishing campaigns spread mainly through malicious emails, fake websites, and suspicious advertisements.[15] The same methods of spreading disinformation were employed during the outbreak of the Zika virus in 2015-2016.[16] At present, cyber attacks were also observed during the COVID-19 pandemic, where social engineering techniques have taken several forms:

Phishing. Phishing is a form of identity theft which targets victims into giving out private and sensitive information such as bank details and passwords through telephone calls, text messages, and emails. The attackers pretend to be tax authorities who will issue tax refunds and help the target individuals cope with the pandemic.[17] In addition, it has been reported that over 4,000 coronavirus-related domains have been registered from January to March this year, three percent of which were considered malicious and five percent were suspicious. Although this seems minimal, cybersecurity firm Check Point stated that "this means that a coronavirus-related domain is 50 percent more likely to be malicious than any other domain registered during the same time period,"[18] and therefore has a high probability to be used for phishing campaigns.

Misinformation. The fear caused by the pandemic created an opportunity for cyber attackers to propagate their schemes. This propels the spread of misinformation, thereby obscuring the proper ways to combat COVID-19 and the right protocols to follow to avoid infection. Fake COVID-19 cures have surfaced which manipulated the vulnerable public's attention and belief.[19] Also, unauthorized fraudulent test kits were being sold online, risking false treatment and detrimental health impacts.[20] Indeed, with the amount of people confined in homes who rely on the internet for pandemic information and updates, misinformation campaigns have gained more ground.

> ***"The government's 12-point national security agenda identified the importance of the informational and cybersecurity goal, which aims to safeguard classified and sensitive government records including state secrets from espionage and to shield the country from cyber attacks that can affect both private and public critical infrastructures."***

Hacking. During the pandemic, hackers were observed to have penetrated health, education, and military sectors. First and most prominent, cyber attacks on healthcare organizations were conducted. According to reports, China-, North Korea-, and Russia-backed hackers target COVID-19 vaccine firms to steal data and gather intelligence on vaccine research.[21] Hacking can also take the form of cyber espionage which is conducted to gain information on measures to combat the virus. State-backed actors operate covertly to obtain information on the capabilities of other states and on the development of potential drugs that can end the pandemic. Aside from this, states can also conduct cyber sabotage, corrupting software and operating processes to weaken an economic or political system, thus resulting to a more tense situation.[22] In the domestic setting, Philippine cyberspace has been breached in education and military sectors.

For the past months, there have been reports of "Zoom bombing" incidents where malicious and obscene materials were projected to students during online classes.[23] Student portals were also hacked, putting student information at risk.[24] Also notable is the continuous hacking operations to Taiwanese and Philippine militaries for several years,[25] which signal the prioritization of geopolitical competition over the global health crisis. For instance, a Chinese APT group called Naikon has been in a five-year cyber espionage campaign in Southeast Asia, stealing geopolitical intelligence in countries near the South China Sea (SCS).[26] The group emerged in 2015 and has been absent for the past years until now, quietly developing their skills to evade detection. Naikon orchestrates government-to-government attacks to gather intelligence on countries through the servers and infrastructure of its victims.[27] In all, the pandemic has presented hackers additional opportunities in multiple fronts.[28]

The current trend of cyber security attacks can be explained by several factors. *First* is the heightened dependency of society on digital infrastructure as the world is put on lockdown.[29] On working-from-home, private IT devices are often less safe compared to those at the workplace that enjoy institutionalized protection. *Second* is the increasing insecurity of the population and their need for information during the pandemic,[30] which eventually led to mass hysteria and huge uncertainty on finding accurate and reliable information online.[31] *Third*, cyber attackers feed on people's fear of the virus to exploit their vulnerable state, thereby creating psychological effects. Notably, the effectiveness of any targeted cyber attack increases with the presence of fear.[32] *Finally*, there was a race among state powers to become the first to find a COVID-19 vaccine and "save" the world.[33] Recently, with the availability of approved vaccines and some in their final stages of completion, this factor proved trivial as different countries claim different narratives. Also, the focus was not fixated on which country created a vaccine first, but on which country could provide vaccines for people other than their own.

These cyber threats and their causes merit an effective response from the government. In this regard, cyber defense complements cybersecurity in reducing vulnerabilities and risks in cyberspace, and in assuring a safe domain for personal and professional undertakings.

"Cyber defense complements cyber security in reducing vulnerabilities and risks in cyberspace, and in assuring a safe domain for personal and professional undertakings."

Cyber Defense in the Philippines

As the WHO encouraged governments to employ science and facts in addressing the pandemic, the Department of Science and Technology (DOST) and the Department of Information and Communications Technology (DICT) implement various science, technology, and innovation (STI) initiatives through a multi-sectoral collaboration. Most notable are technological initiatives such as artificial intelligence-powered thermal scanner system, online portals on COVID-19 and working remotely, free internet connectivity in COVID-19 facilities, and webinars on cybersecurity awareness. The AI-based thermal scanners are mounted in drones and station bays for easier temperature checks of people in queue and limit exposure of medical personnel to possibly infected people. The online portal on COVID-19 (www.covid19.gov.ph) is a platform where the public can access reliable information such as the current figures of infected individuals, programs of the national and local governments, and communication services; whereas the portal on working from home (wfh.gov.ph) is valuable to government employees who are still adjusting to a more virtual work arrangement. The website provides free use of professional tools, learning materials on cybersecurity, and training materials for the enhancement of skills.[34]

These initiatives have been noticed by cyber criminals and are targeted for the conduct of malicious acts. With this, one area that the Philippines must focus its efforts and resources on is cyber defense. In this paper, cyber defense will be defined as "a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks."[35] As the lead on cyber defense, the Department of National Defense (DND) has the responsibility of: a) defending the country, most especially the military network, from cyber attacks; b) securing national security and military systems; c) gathering foreign cyber threat intelligence and determining attribution; d) supporting the national protection, prevention, mitigation of, and recovery from cyber incidents; and e) investigating cyber crimes under military jurisdiction.[36] This mandate can complement the DND's role in the Inter-Agency Task Force for the Management of Emerging Infectious Diseases. Accordingly, it serves as a foundation for the DND's response to the cyber situation amid COVID-19:

The Department of National Defense (DND), in its capacity as the lead on cyber defense, has the responsibility to respond to phishing, misinformation, and hacking activities during the pandemic.

> *On phishing*. Although this threat is imposed more towards the civilian population, cyber attackers target all vulnerable networks. Thus, the DND can ensure that military networks are defended from phishing campaigns and that the administrators operating and monitoring the military network must be equipped and experienced on cyber defense. To this end, the DND can maximize its relations with security and defense partners such as Japan, to which the Philippines is currently considering cooperation on building cyber defense and security infrastructure.[37]
>
> *On misinformation*. Cyber defense serves the purpose of protecting, preventing, and mitigating cyber incidents. With this, the DND can curb the spread of fake information through providing support to the DICT in its functions such as on public awareness campaigns and on defending systems against the creation and proliferation of fraudulent websites, infographics, and social media posts on COVID-19.

On hacking. The DND can continuously develop its foreign cyber threat intelligence capabilities to: a) respond decisively after hackers infiltrated government and military systems; and eventually, b) prevent state-backed or individual hackers to gather critical information on the country's COVID-19 response, as well highly confidential information on national security.

Points of Consideration

The realization of these cyber defense measures is challenged by several issues:

Absence of an official definition on cyber defense. The Philippines has no official definition of cyber defense. Although the term is mentioned in key government documents such as the National Cybersecurity Plan (NCSP) 2022 and the National Defense Strategy (NDS) 2018-2022, it remains unclear how the Philippines defines cyber defense. This hinders the fulfillment of the country's cyber goals as cyber defense serves to prevent, detect, and provide timely responses to cyber threats and attacks on critical public and private infrastructures.[38] Plans on cyber defense will remain afloat without a strong and well-established cyber defense definition. With this, addressing the complexity of cyber attacks during COVID-19 becomes a challenge.

Weak collaboration between the government and the civilian population. If the government already struggles to address the health and economic effects of COVID-19, is there a possibility that the pandemic's effects to cyberspace still be focused upon? In this regard, cooperation between the government and the public becomes more crucial. The weak collaboration between the government and the civilian population – as a result of transparency, accountability, and trust issues of the latter to the former – is one hurdle that must be leaped across if the Philippines is truly committed to address the situation.[39] Under a cyber perspective, the pandemic has shown that cyber attackers exploit every vulnerability that they can find, most especially with private technological devices that are used for work-from-home arrangements. Although it is a difficult task to respond to all the issues that the pandemic has brought at the same time, it is the responsibility of the government to educate its citizens to avoid being a target of cyber attacks. Likewise, civilians have a duty to be aware and protect their devices accordingly.

Prioritization of other issues over cybersecurity. As the Philippines grapples with internal and external security issues such as insurgency and territorial integrity, threats in physical space have often been prioritized more over those in cyberspace. This can be explained in three points: a) The concept of cyberspace emerged not until the late 20th century; b) People are more concerned with physical attacks because they are perceived to be more deadly and harmful compared to cyber attacks; and c) Not all states have the advanced technological capability to address cyber issues and develop cybersecurity measures. While these are valid, the depth and intensity of how cyber attacks have been perpetrated over the years must not be overlooked. Cyber attacks might not directly affect people physically but people's critical information and privacy are jeopardized, and this can be more disruptive at times.[40] It is vital that the Philippine government has invested on digital infrastructure across education, health, and defense sectors for the 2021 proposed national budget.[41]

Policy Recommendations

In going forward, both the opportunities and challenges in enhancing the Philippines' cyber capability must be considered. The following recommendations aim to contribute to a robust policy-making on cyberspace, with a focus on cyber defense:

Strengthen cyber defense plans in military modernization. The Revised Armed Forces of the Philippines (AFP) Modernization Program "is the policy of the State to modernize the AFP to a level where it can effectively and fully perform its constitutional mandate to uphold sovereignty and preserve the patrimony of the Republic of the Philippines."[42] The current trend on cyber threats brought by the pandemic must place cybersecurity as a core security concern of the military modernization program.

***Explore regional and international cyber defense collaborations*.** Collective effort in addressing cybersecurity challenges is challenging because states have different national interests and different technological capabilities, which can lead to a different prioritization of cyber threats.[43] With this, collaborations on cyber defense, a common strategic interest with partners such as Australia and Japan, can benefit the Philippines tremendously,[44] most especially in a post-COVID-19 setting.

***Consider cyber terrorism in cyber defense plans*.** The NSS noted that ending all internal armed conflicts, violent extremism, and terrorism remains to be a top security concern. Given the Philippines' long-running terrorist threat and the boundless possibilities in cyberspace, the government must leverage its actions to thwart any acts of cyber terrorism. In 2019, the Philippine National Police Anti-Cybercrime Group (PNP ACG) reported that a Philippine-based website owned by an American was linked to a mass shooting in the US as the site contains racist posts that may trigger someone to carry out deadly attacks.[45] Instances like this affirms the urgency to address the situation, most especially now that the pandemic created a more vulnerable society and global terrorist organizations such as the Islamic State (IS) utilizes the power of social media and the Internet in recruiting new members to carry out deadly attacks.

> ***Although the Philippines has more to develop in its cyber capability, the government must endeavor to be multiple steps ahead to ensure a secure cyberspace that can be sustained even beyond the COVID-19 pandemic.***

***Review the NCSP*.** The inclusion of a cyber defense definition must be considered, and the cyber defense plans of the government must be elaborated to include evaluation and assessment of the cyber threat landscape during the pandemic.

***Continue multi-sectoral collaboration among government and non-government institutions*.** During the Cyber Attack Manila conference in 2019, DND Undersecretary Cardozo Luna stated that the defense establishment has been partnering with technology companies to better understand the threats posed by cyber attacks that target critical infrastructure.[46] This must continue not only in anticipation of cyber attacks but also in contributing to eradicate COVID-19.

***Foster a tech-savvy society*.** A case study suggested that collaboration among the public, private, and civil sectors, specifically the participation of a thousand software developers, led to Taiwan's success in combatting the coronavirus. In fact, in the beginning of March, Taiwan has already launched 59 map systems, 21 line applications, three chat bots, 23 mask sales location search systems, 22 apps, five audio systems, two information sharing systems, and one online mask reservation system. This reinforces the role of technology during a pandemic.[47]

Conclusion

The COVID-19 pandemic did not only catalyze a global health emergency but also raised a cybersecurity alarm.[48] This paper has noted that the cyber threat landscape has not significantly changed during the COVID-19 pandemic, but has merely taken a new form because of latest technological advancements. In comparison to situation before the pandemic, cyber attackers viewed the COVID-19 pandemic as a special opportunity to pursue their activities as people and networks have proven to be more vulnerable in this setting. Cyber criminals continuously adapt their activities as the pandemic progresses. In this regard, prevention and detection are crucial in cyberspace. Together with providing timely responses to cyber incidents, these three courses of action render cyber defense as a powerful tool for a country's cyber domain. Although the Philippines has more to develop in its cyber capability, the government must endeavor to be multiple steps ahead to ensure a secure cyberspace that can be sustained even beyond the COVID-19 pandemic.

# # #

***Christine Lisette M. Castillo** is a Training Specialist 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] World Health Organization, "WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)," January 30, 2020, https://www.who.int/director-general/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov).

[2] World Health Organization, "Coronavirus disease (COVID-19)," October 12, 2020, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19.

[3] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020," March 11, 2020, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

[4] World Health Organization, "WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)," January 30, 2020, https://www.who.int/director-general/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov).

[5] Interpol, "INTERPOL report shows alarming rate of cyberattacks during COVID-19," August 4, 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[6] Johannes Wiggen, "The impact of COVID-19 on cyber crime and state-sponsored cyber activities," *Konrad-Adenauer-Stiftung* No. 391 (2020): 2.

[7] World Health Organization, "WHO reports fivefold increase in cyber attacks, urges vigilance," April 23, 2020, https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

[8] Catalin Cimpanu, "FBI says cybercrime reports quadrupled during COVID-19 pandemic," *Zero Day,* April 18, 2020, https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/.

[9] The Software Alliance. COVID-19 and Cyber Threats in Southeast Asia. 6.

[10] Rappler, "Phishing is top PH cybercrime during pandemic – authorities," July 12, 2020, https://r3.rappler.com/nation/266364-phishing-top-ph-cybercrime-during-pandemic.

[11] National Security Council, *National Security Policy 2017-2022,* 17.

[12] Ibid., 25.

[13] National Security Council, *National Security Strategy 2018.* 13.

[14] Ibid., 15.

[15] Trend Micro, "Social Engineering Watch: Ebola Virus Being Used as Bait to Lure Victims," October 20, 2014, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/social-engineering-ebola-virus-being-used-to-lure-victims.

[16] CyberPeace Institute, "A Brief History of Cyberattacks: From Ebola to COVID-19," March 26, 2020, https://cyberpeaceinstitute.org/news/2020-03-26-a-brief-history-of-infodemics-from-charlie-hebdo-to-ebola-and-covid-19/.

[17] Francois Mouton and Arno de Coning, "COVID-19: Impact on the Cyber Security Threat Landscape," *Research Gate* (2020): 8-9.

[18] Sara Morrison, "Coronavirus email scams are trying to cash in your fear," *Vox,* March 5, 2020, https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams.

[19] Mouton and de Coning, "COVID-19: Impact on the Cyber Security Threat Landscape," 8.

[20] US Food and Drug Administration, "Beware of Fraudulent Coronavirus Tests, Vaccines, and Treatments," https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments.

[21] Gordon Corera, "Coronavirus: Hackers targeted Covid vaccine supply 'cold chain'," *BBC News,* December 3, 2020, https://www.bbc.com/news/technology-55165552.

[22] Wiggen, "The impact of COVID-19," 6.

[23] Jane Kingsu-Cheng, "PARENTS BEWARE: Zoombombers insert obscene materials into grade school online class," *Manila Bulletin,* September 18, 2020, https://mb.com.ph/2020/09/18/parents-

beware-zoombombers-insert-obscene-materials-into-grade-school-online-class/.

[24] Jaehwa Bernardo, "PUP, FEU student portals hacked," *ABS-CBN News,* June 18, 2020, https://news.abs-cbn.com/news/06/18/20/pup-investigating-reports-of-compromised-student-portal.

[25] Catalin Cimpanu, "Hackers target the air-gapped netwoeks of the Taiwanese and Philippine military," *Zero Day,* May 15, 2020, https://www.zdnet.com/article/hackers-target-the-air-gapped-networks-of-the-taiwanese-and-philippine-military/.

[26] ABS-CBN News, "PH target of 10-year Chinese cyber espionage: group," *ABS-CBN News,* May 20,2015, https://news.abs-cbn.com/nation/05/20/15/ph-target-10-year-chinese-cyber-espionage-group.

[27] James Henderson, "Hackers target ASEAN governments during 5-year 'cyber espionage campaign,'" *Channel Asia*, May 13, 2020, https://sg.channelasia.tech/article/679659/hackers-target-asean-governments-during-5-year-cyber-espionage-campaign/ (accessed June 20, 2020).

[28] Bill DeLisi, "The future of hacking: COVID-19 shifting the way hackers work and who they target," *Security Magazine,* August 14, 2020, https://www.securitymagazine.com/articles/93086-the-future-of-hacking-covid-19-shifting-the-way-hackers-work-and-who-they-target.

[29] Mouton and de Coning, "COVID-19: Impact on the Cyber Security Threat Landscape," 5.

[30] Wiggen, "The impact of COVID-19," 3.

[31] Mouton and de Coning, "COVID-19: Impact on the Cyber Security Threat Landscape," 1.

[32] Morrison, "Coronavirus email scams," https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams.

[33] Kate O'Flaherty, "U.S. Warns Chinese Hacking Poses 'Significant Threat' To COVID-19 Response," *Forbes,* May 14, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/05/14/usgovernment-warning-chinese-hacking-poses-significant-threat-to-covid-19-response/#614db72c403b.

[34] Commission on Science and Technology for Development, "Philippines' Initiatives Relative to COVID-19," 2020.

[35] Techopedia, "Cyber Defense," https://www.techopedia.com/definition/6705/cyber-defense.

[36] Department of Information and Communications Technology. Cybercrime Investigation and Coordination Center. *National Cybersecurity Plan 2022.* 18-19.

[37] The Japan Times, "Philippines eyes partnership with Japan on cyber defense and drones," October 13, 2020, https://www.japantimes.co.jp/news/2020/10/13/national/philippines-eyes-partnership-japan-cyber-defense-drones/.

[38] Techopedia, "Cyber Defense," https://www.techopedia.com/definition/6705/cyber-defense.

[39] Michael Beltran, "The Philippines' Pandemic Response: A Tragedy of Errors," *The Diplomat.* May 12, 2020, https://thediplomat.com/2020/05/the-philippines-pandemic-response-a-tragedy-of-errors/.

[40] Nicholas Davis and Algirde Pipikaite, "What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack," *World Economic Forum,* June 1, 2020, https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/.

[41] Department of Budget and Management. *2021 People's Proposed Budget.* https://www.dbm.gov.ph/images/pdffiles/2021-Peoples-Proposed-Budget.pdf.

[42] Department of National Defense, *Issuing the Implementing Guidelines Rules and Regulations of the Revised Armed Forces of the Philippines Modernization Act,* 1.

[43] Forrest Hare, "The Cyber Threat to National Security: Why Can't We Agree?" *Conference on Cyber Conflict Proceedings,* 2010: 212.

[44] Mark Manatan, "Can the Philippines and Australia Elevate their Partnership to a Strategic Level?" *The Diplomat*, August 16 2019, https://thediplomat.com/2019/08/can-the-philippines-and-australia-elevate-their-partnership-to-a-strategic-level/.

[45] Christopher Lloyd Caliwan, "PNP beefs up 'cyber-patrolling' vs. terror attacks," *Philippine News Agency,* August 14, 2019, https://www.pna.gov.ph/articles/1077815.

[46] Phoebe Magdirila, "Philippines prioritizing cybersecurity in defense policy, official says," *S&P Global Market Intelligence*, August 29 2019, https://www.spglobal.com/marketintelligence/en/news-insights/trending/by7iqqevsk488mgzw7nkua2.

[47] Knowledge@Wharton, "Taiwan's Tech-savvy Citizens Helped Flatten COVID-19 Curve," *The Wharton School of the University of Pennsylvania*, July 27, 2020, https://knowledge.wharton.upenn.edu/article/taiwans-tech-savvy-citizens-helped-flatten-covid-19-curve/.

[48] Taylor, Derrick Bryson, A Timeline of the Corona Virus, The New York Times, 13 February 2020. Retrieved from https://www.nytimes.com/article/coronavirus-timeline.html.