NDCP Executive Policy Brief

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

26 June 2020
No. 2020-02

Cyberspace as the New Domain for Great Power Competition: Strengthening the Philippines' Cyber Capability in a Complex Security Environment

Christine Lisette M Castillo

Introduction

The concept of national security has evolved partly due to tremendous technological innovation in the 21st century. On one hand, computer networks enabled businesses and government institutions to do efficient data-sharing and conduct of affairs. From 2000 to 2010, global internet usage grew by 400%.[1] Ultimately, the interconnectedness of people in online communities brought them together to interact in a new domain that is known as cyberspace.[2] On the other hand, the use of cyberspace has created substantial risks and challenges. The Center for Strategic and International Studies (CSIS) published a 45-page list of significant cyber attacks to government agencies and defense and high-technology companies since 2006.[3] This underscores two things: first, there is an increasing dependence on cyberspace in the conduct of day-to-day affairs; and, second, as much as it created more opportunities, cyberspace also facilitated a highly vulnerable society, one that is insecure and unaware. This gap, together with the advantages of operating in this domain, made states recognize the need for greater capability for cyberspace operations,[4] hence prompting great powers to compete for cyber control and dominance.

The United States (US) and China are currently two of the most powerful states in political, military, and economic terms.[5] As the rise of China in recent decades continues to threaten the US as the global hegemon and regional power in the Asia-Pacific,[6] this dynamic has created a risk for regional peace and stability and global order.[7] The great power competition between the US and China has also placed the Philippines in a critical position, having developed close relations with both countries. Thus, this paper aims to discuss how great power competition in cyberspace affects the Philippines. Also, it aims to establish the connection between cyber rivalry and the current Corona Virus Disease 2019 (COVID-19) pandemic. In particular, it seeks to answer the following questions: 1) How is cyberspace utilized by great powers?; 2) How can the Philippines strengthen its cyber capability amidst great power competition?; and 3) What are the implications of the COVID-19 pandemic to the cyber strategies of great powers?

Great Power Competition in Cyberspace

Cyberspace will serve as a strategic platform for the US and China to advance their national and foreign policy interests. Their competition takes place in two key areas: military and economic.

Military. Great powers were compelled to develop capabilities in computer network operations because of two reasons: (1) the significant disadvantages that result from sophisticated cyber-attacks;[8] and (2) the competition for military dominance.[9] In the last two decades, cyberspace has been utilized by states for military operations such as espionage, sabotage, and subversion against adversaries.[10] For the US, military domination in cyberspace was enshrined in two documents, namely, the International Strategy for Cyberspace 2011 and the Department of Defense Strategy for Operations in Cyberspace in 2011. For China, the

Produced 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

goal of increasing its military capability was reflected in its National Defense in 2010 and the 2006-2020 State Informatization Development Strategy documents.[11] Thus far, the US remains as the world's most powerful state in terms of military assets. However, the future does not guarantee the same. If China's economy continues to grow and a portion of this is allocated to military forces, it will become a worthy opponent to the US military. Historically, no dominant power readily gives up its position to a rising challenger;[12] thus, conflicting relations between the US and China will likely continue in the coming decades.[13]

As the US intends to prevent China from challenging its hegemony, the US closely monitors China's military modernization programs and prepares accordingly "to ensure that US interests and allies, regionally and globally, are not negatively affected."[14] The unparalleled military capabilities of the US, as shown in the 1991 Gulf War and the 2003 invasion of Iraq, relied heavily on information technology (IT), "particularly superior command, control, and communications; intelligence collection, surveillance and reconnaissance and logistics, transportation, and administration."[15] This proves the value of cyberspace in conflict operations. Given both the utility and vulnerability that cyberspace provides, adversaries will inevitably seek for ways to challenge the US.

Although cyber capabilities of states are mostly classified, there are evidences of growing military competition between the US and China in cyberspace.[16] Cyber-attacks targeted at each other demonstrate a growing competition.

The first cyber-attack is the 1999 North Atlantic Treaty Organization (NATO) bombing campaign against Yugoslavia. Instead of hitting the original target, the five laser-guided bombs hit the Chinese Embassy in Belgrade which damaged the building and killed three embassy employees. US officials issued a number of apologies, stating that it was a failure in US intelligence and targeting procedures. As a response, Chinese hackers attacked US government and civilian websites, including that of the White House. This confirmed the vulnerabilities of US cyber-based systems and exposed a weakness that other states can exploit. It also resulted to the emergence of the Honkers Union of China, a patriotic hacking group that was also responsible for attacks against Indonesia and the Philippines.[17]

The second cyber-attack case was sparked by the collision between a US Navy EP3 aircraft and a Chinese J-8II fighter in Hainan Island, China in 2001 which led to the death of a Chinese pilot. Together with the embassy bombing two years prior, this triggered weeks of cyber-attacks between American and Chinese hackers, deleting a significant amount of data of private companies and defacing government and private websites. The most prominent among the attacks is the Code Red worm which originated from a university in China and cost an estimated US$ 2.6 billion worth of damage to the US. The cyber attacks intensified as competition in cyberspace escalated.[18]

A distinct pattern can be noted in the great power competition for military superiority in cyberspace: if one conducts cyber-attacks, the other retaliates, and this dynamic is repeated. China has long intended to engage in a military competition with the US through developing capabilities for cyber network operations. The surge of attacks that the US has sustained from China, together with the necessity to maintain military dominance in cyberspace, forced the US to militarize cyberspace and create the US Cyber Command (USCYBERCOM) in 2009. Some argue that it was a necessity yet a disorientation of the US government on the threats and opportunities that military operation in cyberspace entails.[19]

Economic. Competition in cyberspace will not only be military in nature, but also economic. The economy of a state is vital to its military force that a crippled economy means a crippled military as well.[20] Since US military superiority relies both on its economic scale and technological superiority, China develops its cyber strategy in a way that will weaken US military capabilities.[21] In the era of high-technology international commerce, China brings forward its status as the second largest economy in the world to challenge US supremacy. It conducts cyber-enabled economic warfare to steal intellectual property and target almost every sector of the US economy. Notably, China's

Produced 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

strategy is to rob, replicate, and replace: rob the intellectual property of a US company, replicate the technology, and replace what has been stolen from the US company in the Chinese market, and eventually, in the global market.[22] The US Department of Defense reported that 90% of economic espionage cases from 2011 to 2018 involve China.[23] Each case is directed towards leading China for supremacy at American expense, costing the US economy as much as US$ 600 billion per year.[24] Led by China, cyber economic espionage has indeed escalated.[25]

Originally, China's economic espionage program relied on domestic activities such as communications monitoring and human collection until its cyber capabilities had a broader, global reach. This program began when then Chinese leader Deng Xiaoping decided to let foreign manufacturing companies to operate in China.[26] There are also reasonable grounds for China's illicit acquisition of advanced technology from the US.[27] For instance, China's J-20 fighter plane has striking similarities to the F-22 Raptor made by Lockheed Martin, the same company where a Chinese national was accused of stealing technical data.[28] Likewise, a state-owned aerospace company in China was developing turbofan jet engines for commercial aircrafts at the same time that a team of Chinese intelligence officers hacked a French aerospace manufacturer and US companies that do the same.[29] The covert economic activities have direct implications for the US military.

In addition, the cyber espionage activities that originated from China are parallel to China's five-year economic plans. The strategy of stealing intellectual property has led China to become the leading practitioner of economic espionage in cyberspace.[30] Remarkably, Chinese officials tolerate these activities to the point that hacking has been a business practice in China.[31] However, China is not invincible in cyberspace. The lack of a comprehensive protection for intellectual property in China makes it a viable target.[32] This is in comparison with the US where intellectual property laws are strongly enforced and where cyber actions are focused on the competitor's official government activities and not on economic espionage. Nevertheless, cyber economic espionage provides China an advantage in understanding US intentions, strategies, and capabilities.[33] The head of the Federal Bureau of Investigation (FBI) affirmed that China's economic aggression and relentless theft of US assets position China to challenge the US as the world's superpower.[34]

In sum, the complex security environment facilitating great power competition prompts smaller states to develop their cyber capabilities. This is a matter of urgency especially for the Philippines, which has complicated relations with both the US and China.

Philippine Cyber Capability and Dynamics in Asia-Pacific Region

One of the key areas of the US and China's competition is control over the Asia-Pacific. China is arguably a major power in the region that seeks to preserve its periphery from threats. This goal, however, conflicts with the interests of other regional powers such as Japan, South Korea, and India, making it difficult for China to fulfill its interests.[35] The US is also a prominent power in the region bolstered by its alliances and security arrangements with Japan, South Korea, Australia, Singapore, Thailand, and the Philippines.[36] Aside from the aim of maintaining its relations, the US aspires to remain uncontested in terms of military power in the Asia-Pacific. Moreover, the region holds much economic importance to the US as it ensures mutual economic prosperity with other regional states. Thus, it is in the US' best interest to maintain and advocate for economic openness in the Asia-Pacific.[37]

Relatively, the region is a flashpoint for cyberspace. In addition to the booming IT industry, the Internet creates economic opportunities for rapidly growing Asian economies. An escalation of the great power competition in cyberspace will bear consequences for the entire region. Due to the uncertainty of the cyber domain, norms are yet to be agreed upon and there is a risk of misidentifying an espionage exploit as a military action, and cyber conflict can be miscalculated. Notably, the cyber powers in the region such as Russia, Taiwan, North and South Korea, and Australia are struggling to adjust their policies and practices.[38]

Produced 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

The Philippines, as a smaller state, bears a greater burden. First, the great powers are also cyber powers that are capable of carrying cyber-attacks. This is a close concern for the Philippines, having ranked 4th globally with the highest number of online threats in 2019.[39] The country also seems to be a hacker's favorite, with countless hacking incidents over the years involving banks and government websites.[40] Although these hacking incidents are rooted domestically, they expose the vulnerability of Philippine cyberspace, most especially against a technologically-advanced region.

Second, the Philippines has a complex relationship with the US and China. The current Philippine administration shifted its foreign policy away from a longtime ally, the US, in favor of China. This is reflected in Philippine President Rodrigo Duterte's five visits to China from 2016 to 2019[41], increased economic activities between the two countries, promotion of closer ties as exemplified in presidential speeches, and possible abrogation of the Visiting Forces Agreement (VFA) with the US, among others. However, China is considered as one of the biggest cyber offenders. From 2006 to 2018, China has been involved in 108 cyber incidents, including cyber espionage in 12 countries and information theft.[42] More importantly, infamous advanced persistent threat (APT) groups linked to China are considered the world's oldest, most skilled, and most active agents of cyber espionage.[43]

Developments in the South China Sea (SCS) further complicate the volatile security environment. The SCS has been a place for China to extend its influence, power, and cyber capabilities. 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 SCS.[44] 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.[45] At present, the Philippines seems to be at a crossroads, having fought in the previous years for its rights in the disputed waters but relegating its claims to lower level priorities in the current administration.[46] As Duterte said in his State of the Nation Address in 2019, "The West Philippine Sea is ours, but we have to temper the times and the realities we face today."[47] Nevertheless, threats to the Philippine cyberspace must not be taken lightly.

Cybersecurity experts believe that cyber espionage in the Philippines will not recede any time soon.[48] This is grounded on two factors: first, the Philippines' capability to deter cyber espionage activities or be proactive in one is still lacking, thus making the country a prime target; and second, in consideration of the former, today's geopolitical climate presents a very challenging situation for the Philippines, most especially if put alongside China in both issues of maritime dispute and cybersecurity. In this context, there are strategic actions that the Philippines must take to strengthen its cyber capability.

First, it must boost its IT infrastructure system for reconnaissance, intelligence, and prevention or early detection of cyber threats that can undermine national security. Major focus areas include the SCS and protection of critical information infrastructure.

Second, there is a need for more robust education and training programs on cybersecurity to civilian and military personnel. This will enable the cybersecurity workforce to grow and develop.

Third, the Philippines must leverage partnership building through domestic, bilateral, and regional collaborations. This includes collaboration among the government, private sector, academe, and non-profit organizations. Also, engaging in cyber intelligence capacity-building with partners such as Australia and Japan is an opportunity that the Philippines must pursue.[49]

Finally, the Philippines and the US must pursue a review of the Mutual Defense Treaty (MDT) to include cyberspace as a domain of security concern. The MDT, which was signed in 1951, is the foundation of the two countries' alliance. As cyber espionage activities that are aimed to gather intelligence on the SCS are prevalent, the treaty fails to provide assurance

Produced 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

on the US' commitment to defend and protect the Philippines, particularly the West Philippines Sea (a portion of the SCS that the Philippines claims), in the occurrence of a cyber-attack.[50] The Philippines' Secretary of National Defense Delfin Lorenzana stressed the urgency of the MDT review as tensions in the SCS continuously threaten Philippine national security.[51]

Strengthening the Philippines' cyber capability also proves to be necessary in the current health crisis, where evident great power competition in cyberspace continues.

Cyber Strategies of Great Powers Amid the COVID-19 Pandemic

The boundless nature of cyberspace makes its utility boundless as well. This domain is not only important in the military and economic aspects of the great power competition but also in the context of the COVID-19 pandemic. The virus, from a newly identified coronavirus SARS-CoV-2, is an infectious disease that originated from Wuhan City, China in December 2019.[52] The spread of the virus in over 200 countries has disrupted government systems and people's everyday affairs.[53] The emerging 'new normal' during the COVID-19 pandemic prompted people to stay indoors and spend more time on the Internet.

The success stories of countries in COVID-19 response highlight the necessity of technological capability to combat the pandemic. Asia-Pacific countries such as China, South Korea, Singapore, and Japan actively deploy technology "to collect data on the virus's progress and efforts to contain it, including tracking those who are infected and their contacts."[54] Most of these efforts involve mobile apps for contact tracing. In particular, South Korea's quick and effective response was powered by its surveillance technology and transaction data. The South Korean government repurposed the massive amount of information it has collected to trace people's transactions and integrate multiple forms of digital information.[55] Singapore also provides a great example of using information and communications technology (ICT) for rapid and large-scale contact tracing through digital footprints.[56]

Meanwhile, China has integrated its contact tracing and quarantine enforcement applications to the messaging application WeChat.[57] Central to the US' efforts is the development of a vaccine called AZD1222. The US Department of Health and Human Services (HHS) partnered with AstraZeneca, a British-Swedish multinational biopharmaceutical company to develop and conduct clinical testing of the AZD1222 which uses a vaccine platform technology for large-scale production. HHS Secretary Alex Azar stated that providing a vaccine to the American public as soon as possible will safely reopen the country and bring life back to normal.[58]

Aside from these technological efforts, cyberspace has become a tool for great powers to manipulate the pandemic and advance their respective interests. State-linked cyber criminals have taken advantage of the pandemic.[59] In May, the US accused China-linked cyber actors of stealing COVID-19 research on vaccines and treatments.[60] According to the US Cybersecurity and Infrastructure Security Agency, the incident poses a significant threat to the US' response to the virus. China's Foreign Ministry spokesperson Zhao Lijian denied the accusation by stressing that "China is a staunch upholder of cybersecurity and a victim of cyber attacks."[61] In support, Hu Xijin, the editor of state media organization the Global Times, stated that the accusation is "in line with the long-term distortion of China's image by the US."[62] The World Health Organization (WHO) noted that there has been a fivefold increase in cyber attacks since the start of the pandemic.[63]

The COVID-19 pandemic has also become a channel for power projection. The US points to China as the place of origin of the virus, with US President Donald Trump referring to COVID-19 as the "Chinese Virus;" whereas China has also set out a narrative that the virus is a US creation, with Zhao Lijian stating that it was the US military who brought the virus to China.[64] Driving this competition is the growing perception that the first country to produce successful vaccines and treatments will be viewed as the "savior" of the world. It will also create a favorable economic impact.[65] Both the US and China have expressed willingness to share to the Philippines any vaccine that will be successfully developed,

Produced 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

stating that the Philippines is an ally of the US and a "friendly neighbor" of China.[66]

Notably, the COVID-19 pandemic is conveniently being used by the great powers to advance their cyber strategies on key security areas. The pandemic has also shown that great powers will assess and adjust to a situation, and always pursue their national interests.

Policy Considerations

In the current geopolitical setting, cyberspace serves as a new domain for great power competition. This will create both opportunities and challenges for the Philippines as a small state in the Asia-Pacific. Several policy recommendations are proposed for consideration.

First, the Philippines must strengthen its cyber capability. In addition to boosting its IT infrastructure system, developing its education and training programs, and pursuing the review of the MDT, collaboration with security partners such as Australia, Japan, and the Association of Southeast Asian Nations (ASEAN) must be highlighted. The ASEAN Smart Cities Network (ASCN), a new platform for ASEAN cities towards a smart and sustainable urbanization, is a tool which can be improved.[67] If smart technologies are central to the ASCN, cities must not only be smart and sustainable, but also secure. Making lives easier through the use of modern IT must not compromise the security of ASEAN countries' cyberspace. The collaboration, however, must not be projected as an encirclement or containment by the US and its allies to China to avoid the risk of conflict escalation.[68]

*Second, w*idespread, systemic cyber-attacks must be anticipated to ensure early and decisive actions. The COVID-19 pandemic has shown that responding to a health crisis is similar to addressing cyber threats. In fact, the occurrence of a "cyber pandemic" in the future is possible.[69] For instance, the 2003 Slammer/Sapphire worm is one of the fastest worms in history which spread to over 75,000 infected devices in just 10 minutes.[70] The spread of virus will be faster as communities grow more dependent on cyberspace. It might not directly affect people physically but their critical information and privacy are jeopardized. In addition, a cyber pandemic might create more economic disruption than what states are experiencing with COVID-19. If millions of devices will be taken offline and the world will experience a cyber lockdown, all businesses, communication, and data transfers will be blocked. It is estimated that a day without the Internet would cost more than US$ 50 billion which means US$ 1 trillion loss for a 21-day cyber lockdown.[71]

Third, the Department of Information and Technology (DICT), as the primary institution for the pursuit of the government's ICT development agenda,[72] must work in close partnership with the Armed Forces of the Philippines (AFP) in innovating cybersecurity measures. The AFP has a vital role not only in securing and defending the country's physical territory but also in ensuring that critical and highly-confidential information on national security will not be obtained by adversaries through cyber espionage.[73]

Fourth, norms for the responsible use of cyberspace must be established among states. The prevalence of cyber-attacks has led various stakeholders to turn to the creation of cyber norms that can "regulate state behavior and limit damages from malicious cyber activity." The development of cyber norms can be done in several processes. Multilateral norm diplomacy involves state to state exchange of cyber norms through organizations such as the United Nations General Assembly. Private norm processes involve private institution to state interaction, with high-profile experts offering recommendations on cyber norms for states. In addition, industry-focused norm processes are industry to industry efforts to identify cyber norms. Finally, multi-stakeholder norm processes incorporate all three processes together, providing an inclusive forum to discuss, identify, and advance cyber norms.[74]

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.[75] However, regional norms in cyberspace are still subject to contestation. This requires a higher level of trust in cyberspace for the effective

Produced 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

implementation of ASEAN's 2020 ICT Master Plan.[76]

In sum, the Philippines must continue to assess viable recommendations to avoid being unnecessarily trapped in the binary choice between the US and China.

Conclusion

With the desire to redeem its past glory, China is employing all necessary options to achieve global hegemony. The rise of China fueled the great power competition in the Asia-Pacific, and ultimately, the world. With states constantly adapting to change, the rivalry between the US and China has also gained a new ground in cyberspace. As much as it provides opportunities, cyberspace has also enabled great powers to conduct illicit operations to achieve their interests. In a liberal world view, states have a natural tendency to cooperate and engage on dialogues about common security issues. This is true for the small states in the international system that cannot rely on their own. But for the great powers who have all the means, the realist world view is more appropriate. Great powers cooperate but it is expectedly in the attainment of their national interests.

With this, the Philippines must capacitate itself and strengthen its cyber capabilities. Russian President Vladimir Putin said that whichever country leads in artificial intelligence by 2030 will rule the world. Although leadership in cyberspace may be too ideal for the Philippines, cyberspace is a domain that is not only for the great powers to utilize but also for the smaller states to explore.

# # #

Christine Lisette M. Castillo *is a Training Specialist at the Research and Special Studies Division of the National Defense College of the Philippines (NDCP).* *For comments and suggestions, please email* christinelisettecastillo@gmail.com.

Endnotes

[1] Colonel Jayson M. Spade, *China's Cyber Power and America's National Security* (Pennsylvania: US Army War College, 2012), 3.
[2] Damien Van Puyvelde and Aaron F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge: Polity Press, 2019), 23.
[3] Center for Strategic and International Studies, "Significant Cyber Incidents," Accessed May 13, 2020, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.
[4] Spade, *China's Cyber Power and America's National Security*, 7.
[5] Robert J. Art, "The United States and the Rise of China: Implications for the Long Haul," *Political Science Quarterly* 125, 3 (2010): 359.
[6] Art, "The United States and the Rise of China: Implications for the Long Haul," 359.
[7] Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "The "Cyber Problem" in U.S.-China Relations," in *Getting to Yes with China in Cyberspace* (Santa Monica: RAND Corporation, 2016), 2.
[8] Francis C. Domingo, "Conquering a new domain: Explaining great power competition in cyberspace," *Comparative Strategy* 35, 2 (2016): 154.
[9] Domingo, "Conquering a new domain: Explaining great power competition in cyberspace," 155.
[10] Domingo, 154.
[11] Ibid.
[12] Art, "The United States and the Rise of China: Implications for the Long Haul," 360.
[13] Art, 359.
[14] United States Office of the President, *National Security Strategy 2010* (Washington, DC: Office of the President, 2010), 43.
[15] Spade, *China's Cyber Power and America's National Security*, 1.
[16] Domingo, "Conquering a new domain: Explaining great power competition in cyberspace," 157.
[17] Domingo, 159-160.
[18] Domingo, 162-163.
[19] Domingo, 161-162.
[20] Samantha F. Ravich, PhD and Annie Fixler, "The Economic Dimension of Great Power Competition and the Role of Cyber as a Key Strategic Weapon," *The Heritage Foundation* (2020): 63.
[21] Ravich and Fixler, 66-67.
[22] Ravich and Fixler, 66.
[23] Ibid.
[24] Ravich and Fixler, 67.
[25] J.D. Work, Trey Herr, and Will Loomis, "Scenario One: Great Power Competition," *Atlantic Council Sowcroft Center for Strategy and Security.*
[26] James Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," *Lowy Institute MacArthur Asia Security Project,* 7.
[27] Ibid.
[28] Ravich and Fixler, "The Economic Dimension of Great Power Competition and the Role of Cyber as a Key Strategic Weapon," 67.
[29] Ravich and Fixler, 66.
[30] Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," 7.
[31] Lewis, 7-8.
[32] Lewis, 8.
[33] Lewis, 9.
[34] Ravich and Fixler, "The Economic Dimension of Great Power Competition and the Role of Cyber as a Key Strategic Weapon," 66.
[35] Ashley J. Tellis, Alison Szalwinski, and Michael Wills, "The Return of U.S.-China Strategic Competition," in *U.S.-China Competition for Global Influence*, (Seattle: The National Bureau of Asian Research, 2019): 7.
[36] Art, "The United States and the Rise of China: Implications for the Long Haul," 384.
[37] Art, 381.
[38] Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," 1-2.
[39] Gabriela Baron, "PH ranks 4th in the world with highest number of online threats," *Manila Bulletin,* March 3, 2020, https://technology.mb.com.ph/2020/03/03/ph-ranks-4th-in-the-world-with-highest-number-of-online-threats/ (accessed June 19, 2020).
[40] Domingo, "Strategic Considerations for Philippine Cyber Security," 6.
[41] Richard Heydarian, "How Rodrigo Duterte's latest Beijing visit marks a crossroads for China, the Philippines and Asia," *South China Morning Post,* September 1, 2019, https://www.scmp.com/news/china/diplomacy/article/3025170/how-rodrigo-dutertes-latest-beijing-visit-marks-crossroads.
[42] Sintia Radu, "China, Russia Biggest Cyber Offenders," *US News,* February 1, 2019, https://www.usnews.com/news/best-countries/articles/2019-

Produced 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

02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows (accessed June 19, 2020).
[43] Scott Ikeda, "New Report Reveals Chinese APT Groups May Have Been Entrenched in Some Servers for Nearly a Decade Using Little-Known Linux Exploits," *CPO Magazine*, April 24, 2020, https://www.cpomagazine.com/cyber-security/new-report-reveals-chinese-apt-groups-may-have-been-entrenched-in-some-servers-for-nearly-a-decade-using-little-known-linux-exploits/ (accessed June 19, 2020).
[44] 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 (accessed June 20, 2020).
[45] 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).
[46] Mark Bryan F. Manantan, "Pivot Toward China: A Critical Analysis of the Philippines' Policy Shift on the South China Sea Disputes," *Asian Politics & Policy* 11, 4 (2019): 644.
[47] Cliff Venzon and Mikhail Flores, "Duterte says South China Sea dispute is 'delicate balancing act,'" *Nikkei Asian Review,* July 22, 2019, https://asia.nikkei.com/Politics/International-relations/Duterte-says-South-China-Sea-dispute-is-delicate-balancing-act (accessed June 29, 2020).
[48] Oliver Samson, "PHL government, firms target of nation state cyber espionage—FireEye," *Business Mirror,* May 27, 2017, https://businessmirror.com.ph/2017/05/27/phl-government-firms-target-of-nation-state-cyber-espionage-fireeye/ (accessed June 21, 2020).
[49] Mark Bryan Manantan, "How to Build a Cyber-Resilient Philippines," *Asia Pacific Pathways to Progress Foundation, Inc.,* July 3, 2019, https://appfi.ph/resources/commentaries/2769-how-to-build-a-cyber-resilient-philippines (accessed June 21, 2020).
[50] Lucio Blanco Pitlo III, "Ambiguity and Changing Times Compel Review of the Philippine-U.S. Mutual Defense Treaty," *Asia Maritime Transparency Institute,* February 8, 2019, https://amti.csis.org/ambiguity-changing-times-compel-review-mutual-defense-treaty/ (accessed June 25, 2020).
[51] David Santos, "Lorenzana renews call to review mutual defense treaty with U.S. after latest tension in PH sea," *CNN Philippines,* June 8, 2019, https://cnnphilippines.com/news/2019/6/8/lorenzana-russia-united-states-warship.html (accessed June 25 2020).
[52] Lauren M. Sauer, M.S., "What is Coronavirus?" *John Hopkins Medicine*, https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus (accessed June 22, 2020).
[53] World Health Organization, "Coronavirus disease (COVID-19) pandemic," https://www.who.int/emergencies/diseases/novel-coronavirus-2019 (accessed June 23, 2020).
[54] Yasheng Huang, Meicen Sun, and Yuze Sui, "How Digital Contact Tracing Slowed Covid-19 in East Asia," *Harvard Business Review,* April 15, 2020, https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia (accessed June 26, 2020).
[55] Justin Fendos, "How surveillance technology powered South Korea's COVID-19 response," *Brookings,* April 29, 2020, https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/ (accessed June 26, 2020).
[56] Knowledge @ Wharton, " Combating COVID-19: Lessons from Singapore, South Korea and Taiwan," April 21, 2020, https://knowledge.wharton.upenn.edu/article/singapore-south_korea-taiwan-used-technology-combat-covid-19/ (accessed June 26, 2020).
[57] Huang, Sun, and Sui, "How Digital Contact Tracing Slowed Covid-19 in East Asia," https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia (accessed June 26, 2020).
[58] US Department of Health and Human Services, "Trump Administration's Operation Warp Speed Accelerates AstraZenica COVID-19 Vaccine to be Available Beginning October," May 21, 2020, https://www.hhs.gov/about/news/2020/05/21/trump-administration-accelerates-astrazeneca-covid-19-vaccine-to-be-available-beginning-in-october.html (accessed June 26, 2020).
[59] Adil Radoini, "Cyber-crime during the COVID-19 Pandemic," *United Nations Interregional Crime and Justice Research Institute,* May 11, 2020, http://www.unicri.it/news/article/covid19_cyber_crime (accessed June 23, 2020).
[60] David E. Sanger and Nicole Perlroth, "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks," *The New York Times,* May 10, 2020, https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html (accessed June 23, 2020).
[61] Helen Davidson, "China hacking poses 'significant threat' to US Covid-19 response, says FBI," *The Guardian,* May 14, 2020, https://www.theguardian.com/world/2020/may/14/china-hacking-poses-significant-threat-to-us-covid-19-response-says-fbi (accessed June 23, 2020).
[62] Davidson, "China hacking poses 'significant threat' to US Covid-19 response, says FBI," https://www.theguardian.com/world/2020/may/14/china-hacking-poses-significant-threat-to-us-covid-19-response-says-fbi (accessed June 23, 2020).
[63] 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 (accessed June 24, 2020).
[64] Bruce Y. Lee, "No, COVID-19 Coronavirus Was Not Bioengineered. Here's The Research That Debunks That Idea," *Forbes,* March 17, 2020, https://www.forbes.com/sites/brucelee/2020/03/17/covid-19-coronavirus-did-not-come-from-a-lab-study-shows-natural-origins/#638be6b3728c (accessed June 30, 2020).
[65] 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/us-government-warning-chinese-hacking-poses-significant-threat-to-covid-19-response/#614db72c403b (accessed June 24, 2020).
[66] ABS-CBN News, "US willing to share COVID-19 vaccine to allies: PH defense dep't," June 14, 2020, https://news.abs-cbn.com/news/06/14/20/us-willing-to-share-covid-19-vaccine-to-allies-ph-defense-dept (accessed June 24, 2020).
[67] Centre for Liveable Cities, ASEAN Smart Cities Network (Singapore: CLC Publications, 2018), 2.
[68] Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," 12.
[69] 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,* https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/ (accessed June 24, 2020). A "cyber pandemic" is a cyberattack that is similar to the coronavirus but will spread faster and further and will have greater, if not equal, economic consequences.
[70] University of California Berkeley Media Relations, "Sapphire/slammer worm shatters previous Internet speed records," February 4, 2003, https://www.berkeley.edu/news/media/releases/2003/02/04_worms.html (accessed June 24, 2020).
[71] Davis and Pipikaite, "What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack," https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/ (accessed June 24, 2020).
[72] Department of Information and Communications Technology, "Republic Act No. 10844," Accessed June 24, 2020, https://dict.gov.ph/about-us/republic-act-no-10844/.
[73] Philippine News Agency, "DND urges military to beef up cybersecurity," April 4, 2019, https://www.pna.gov.ph/articles/1066440 (accessed June 26, 2020).
[74] Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," *Carnegie Endowment for International Peace* (Washington, DC: Carnegie Endowment for International Peace Publications Department, 2020), 2-3.
[75] Candice Tran Dai and Miguel Alberto Gomez, "Challenges and opportunities for cyber norms in ASEAN," *Journal of Cyber Policy* 3, 2 (2018): 1-2.
[76] Tran Dai and Gomez, "Challenges and opportunities for cyber norms in ASEAN," 16.

Produced 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