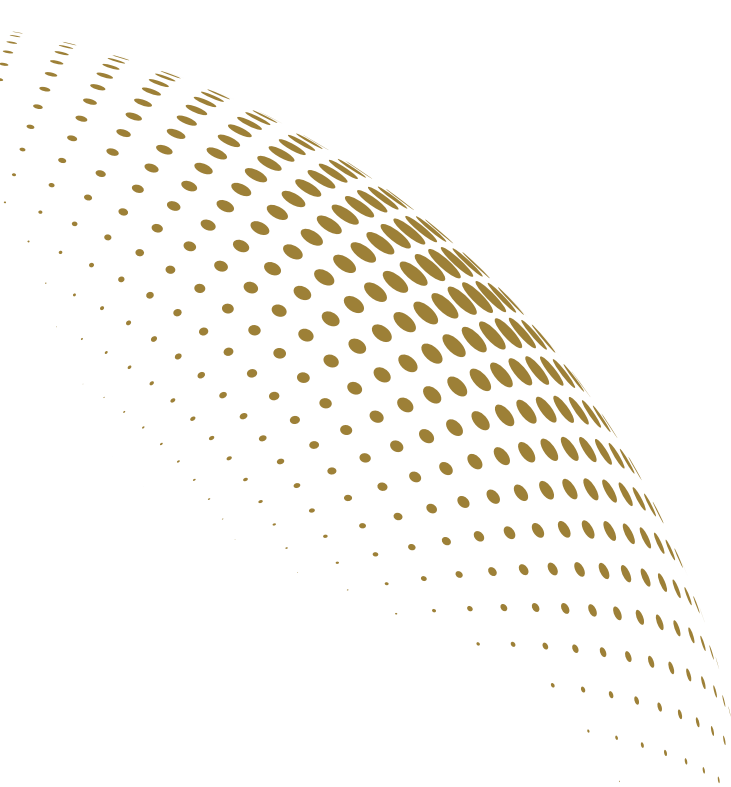




EXECUTIVE POLICY BRIEF

Towards a Cyber Defense Strategy in the Philippines

Christine Lisette M Castillo



27 June 2023
Issue Number 2023-03
EPB ISSN 2945-4689

INTRODUCTION

The National Cybersecurity Plan (NCSP) 2022 was launched in 2017, a year after the Department of Information and Communications Technology (DICT) was established. Certainly, there was an urgency to employ cybersecurity measures that are commensurate with the increasing magnitude of activities in cyberspace as the years progress. However, given the complex nature of cybersecurity and the priority of the DICT on technological development and interconnectivity, challenges still remain in the pursuit of cybersecurity. This pertains not only to institutional challenges but also to the fast-paced changes in the cyber threat landscape that disrupt progress in all relevant sectors. This reality confronts the Philippines at an alarming rate.

The publication of the NCSP 2022 elevated public and policy discussions on cybersecurity. The document provided a context on how the Philippines perceives cybersecurity and how best to approach it. However, as a cybersecurity plan, no comprehensive discussions on cyber defense were included. There arises the necessity for a cyber defense document that will not only guide the defense establishment in protecting vital assets in cyberspace but also in informing key stakeholders and the general public of the commitment to, capabilities on, and the trajectory for cyber defense in the Philippines. Indeed, the creation of a national strategy on cyber defense has been constantly put forward by scholars and academics. As the release of a new government document on cybersecurity by the DICT is expected this year, the potential to formulate a cyber defense document also arises. In this regard, this policy brief intends to provide a way forward for the formulation of a cyber defense strategy in the Philippines. It further aims to contribute to policy discussions on cyber defense and expand the literature on this topic. In particular, this policy brief seeks to answer the following key questions:

- a. Why does the Philippines need a cyber defense strategy?
- b. What are the implications of formulating a cyber defense strategy in the Philippines?
- c. How can a cyber defense strategy be realized?

This policy brief puts forward a multi-level analysis of the challenges and opportunities in cyberspace. By analyzing cybersecurity challenges in the international, national, and individual levels, policy recommendations can be generated to ultimately aid the formulation of a cyber defense strategy in the Philippines.

MAJOR CASE ISSUES

THE NEED FOR A CYBER DEFENSE STRATEGY

The potential power that cyberspace can provide entices actors to exploit the domain. In particular, states that are already powerful and influential in political, economic, military, and other relevant fronts still pursue preeminence in cyberspace. This further reinforces that in the digital era, state and non-state actors are increasingly drawn to cyberspace and all opportunities therein. And while cyberspace is viewed by some as an equalizer¹ among states, those with greater cyber capabilities remain in the more advantageous position. This means that it is more challenging for developing countries in the region such as the Philippines to navigate interests and priorities in cyberspace while dealing with geopolitical challenges. This provides an impetus for the country to highlight cyber defense and employ courses of action towards its development, such as the formulation of a strategy document. Although a cyber defense plan is also important, a strategy must first be formulated before plans can be drawn. From the strategy, all specific plans will be determined.

In particular, the need for a cyber defense strategy is supported by the following points:

geopolitical environment, defense advantage, and digital transformation.

Geopolitical environment. The Indo-Pacific region holds strategic importance in multiple fronts. Aside from the fact that the largest digital economies in the world thrive in the region, great power competition besets the geopolitical environment.² This competition occurs in multiple areas, including cyberspace. Due to this, the Philippines is placed in a critical position as the vulnerability of the country's cyberspace becomes a platform for cyber operations to ensue. The highly-organized and oftentimes state-sponsored cyber operations are usually employed by advanced persistent threat (APT) groups. An example is Lazarus, an APT group of expert hackers tied to the North Korean government. Lazarus was reported to be the mastermind behind the major hacking operation in 2016 which involved the illegal transfer of U.S.\$ 81 million from the account of the Bangladesh Bank in the Federal Reserve Bank in New York to four fictitious accounts in the Rizal Commercial and Banking Corporation (RCBC) in Makati City.³ This incident showed two points: first, it reaffirmed the global effects of cyber attacks which disrupt economic progress and national security; and second, it revealed that the Philippines is deemed as an easy target for these kinds of operations. This vulnerability in cyberspace may affect digital trust on institutions and may discourage interested businesses to invest in the country. Indeed, the country's involvement in the Lazarus heist put a spotlight on the risks of cyber attacks to the financial system.⁴

Naikon is another APT group that has targeted the Philippines. Having originated from China and believed to be government-sponsored, Naikon conducts cyber espionage in Southeast Asian countries to gather geopolitical information on the South China Sea by attacking civilian and government agencies, including military networks.⁵ Naikon conducts a government-to-government approach where, after targeting a country's government institution,

will attack the same country's other government institutions using the information gathered from the first, therefore misdirecting attribution to avoid detection.⁶ With the Philippines' claim on the West Philippine Sea, Naikon's operations certainly impact the country's efforts to pursue its national interests. In all, a cyber defense strategy will aid the Philippines in navigating the geopolitical environment which is plagued by these kinds of threats and attacks from APT groups.

Defense advantage. The defense advantage is another compelling reason for a cyber defense strategy. In a conventional military sense, offensive operations are usually perceived to provide greater advantages than defensive operations. But beyond this notion, the defense advantage or the myth of the offensive puts forward that victory through cyber offense will only be achieved if an attacker has full knowledge of the cyber defense systems of the target and how these operate. This means that the more sophisticated the cyber defense systems of the target are, the more sophisticated cyber offensive capabilities are needed as well.⁷ Given the complexity of this task, there is a higher chance that the attack may prove ineffective.

Aside from this, the myth of the offensive also refutes the notion that cyberspace makes attacking "easier and more cost-effective" and defending "hard and more resource-intensive." This is not always the case, especially if cyber attacks are employed by states with ultimate ends. For instance, the Stuxnet worm cyber attack on the Iranian nuclear enrichment program by the United States and Israel took years to plan and months to execute. The level of sophistication and the amount of resources used to carry out the attack meant that only a cyber superpower, or in this case cyber superpowers, could have pulled it off.⁸

Given these considerations, it is more apt to develop the Philippines' cyber defense at present. More than the capability to disrupt and manipulate others' cyber domains, the

country needs the capability to defend itself from cyber attacks and threats. Aside from the fact that developing and conducting cyber offense is costly and employs sophistication which only a highly-capable state can execute, reality suggests that the current cybersecurity posture of the country is yet to mature. On another note, the defense advantage can also affect how the Philippines pursues its ICT agenda, specifically digital transformation.

Digital transformation. It was reported that Philippine organizations have lost Php 40 million in ransom payments and in recovering from ransomware in 2020,⁹ while a potential economic loss of U.S.\$ 3.5 billion from cyber attacks was predicted.¹⁰ With this precarious situation, alongside the country ranking 4th globally in the most targeted by online threats,¹¹ plans for digital transformation will encounter challenges. In particular, e-commerce activities and the financial technology (fintech) industry have higher chances of being more compromised. The Philippine fintech market valuation has grown to 224% between 2016 and 2021, indicating that Filipinos use one fintech service per second.¹² In part, this shows that the Philippines values e-commerce and the digital economy as “key engines of growth and economic recovery”.¹³ Therefore, cyber attacks directed to e-commerce platforms can significantly destabilize the economy, given that activities such as online shopping have become a major part of life for Filipinos.¹⁴

The development of the e-government program will also be affected. Earlier this month, the government launched the e-Gov PH or the e-Government Philippines Super App as part of its goals for digital transformation. The app, which consolidates government transactions and eliminates red tape, was designed to be a comprehensive platform to benefit Filipinos.¹⁵ A platform for interconnectivity, the app is “a one-stop online system that will minimize economic cost for the citizens”,¹⁶ with features such as online payment, application for passport, viewing of government IDs, registration of

SIM cards, and creation of resume, among others.¹⁷ The app is also in development for travel-related services and visa requirements.¹⁸ On the one hand, the development of the app is a huge success for digital transformation in the country. On the other hand, it can be viewed as another platform for cyber threat actors to exploit if not defended.

In summary, the digital transformation program, alongside the geopolitical environment and the defense advantage, are compelling reasons towards the formulation of a cyber defense strategy in the Philippines. Indeed, with the fast-paced innovation and the cyber threat landscape that the Philippines finds itself in, activities involving cyberspace must be secured, protected, and well-defended. This pursuit can be forwarded through a multi-level analysis of cybersecurity challenges.

A MULTI-LEVEL ANALYSIS OF CHALLENGES IN CYBERSPACE

The levels of analysis that will be used in this paper are the international, national, and individual levels. At the international level, the country is in a critical position with regard to other states’ competing interests in cyberspace. At the national level, the Philippines faces various kinds of cyber threats, particularly cyber espionage. While at the individual level, social engineering techniques endanger Filipinos from meaningful digital participation.

Cyber Conflict: international level

The Indo-Pacific region houses some of the most powerful states in cyberspace such as the United States (U.S.), Japan, China, and Russia.¹⁹ In addition, other highly-capable states in the region develop their cyber capabilities through the establishment of cyber defense agencies, units, or military commands.²⁰ The notion that future wars will most likely be fought in cyberspace, together with the continuous build up of cyber

capabilities, serve as an impetus for competition and conflict in cyberspace.

State competition in cyberspace may result in cyber conflict, one which may not directly involve the Philippines but will create repercussions nevertheless. For instance, a possible cyber conflict between the U.S. and China will impact the country in various ways. On the one hand, the Philippines and the U.S. are long-standing allies. In line with their defense partnership, the Philippines is the largest recipient of U.S. military aid in the entire Indo-Pacific, amounting to Php 57 billion dollars worth of military equipment and training since 2015.²¹ A recent showcase of the two countries' strong alliance is the revitalization of the Enhanced Defense Cooperation Agreement (EDCA) in February 2023 which oversaw the addition of four (4) new EDCA sites for disaster relief, maritime security, and counterterrorism.²² On the other hand, the Philippines also shares close relations with China, with the latter being the largest trading partner and second largest export market of the Philippines. Beyond the South China Sea disputes, both countries benefit economically from their partnership.²³

If a cyber conflict between the U.S. and China truly occurs, there is a possibility that the Philippines may be involved, given that there is already a geopolitical conflict between the two great powers on the South China Sea, which can spill over to cyberspace. Cyberspace then becomes another platform for state and non-state actors to attack rivals and competitors. Moreover, the U.S. concern on China's technological rise facilitated a technology war between the two countries, which may even lead to a global conflict.²⁴ The Philippines, although building its capacity on cyber defense with the help of the U.S., will still struggle to defend its own networks as it cannot always rely on others for help in defending its own.

Cyber Espionage: national level

Intelligence gathering is common among states, especially in determining a

competitor's interests, behavior, and direction. This activity, however, can go beyond common operations to exploitation and threat. Cyber espionage, which was defined by the DICT as the act of using computer networks to illegally access confidential information,²⁵ is related in this regard. Cases of cyber espionage are usually politically-motivated and state-associated.²⁶

The Philippines is being plagued by incidents of cyber espionage that are detrimental to the country's national security. One example is the leak of the transcript of a private conversation between former Philippine President Rodrigo Duterte and former US President Donald Trump in 2017. The transcript included attachments of internal documents from the National Security Council (NSC) and other government documents. APT32 or OceanLotus, an APT group that is tied to the Vietnamese government, was reported to be behind the attack, after being disappointed by the Philippines' warmer ties with China during the former administration. The leak of sensitive government documents suggests that Vietnam conducts cyber espionage to gather information it may use to advance its interests in the region.²⁷

Another example is a hacking campaign perpetrated by the newly-identified hacking group called Dark Pink which likely originated from within the region. It was reported that the group steals data and targets government organizations in Southeast Asia and Europe through phishing and advanced malware. In the Philippines, Dark Pink has specifically targeted the defense and the military.²⁸ Some also advance the argument that the Philippines is one of the targets of Chinese telecommunications giant Huawei who reportedly conducts cyber espionage for the Chinese government. This may be driven by China's aim of not only increasing the competitiveness of Chinese companies in the global market through 5G technology but also asserting more dominance and power in the region.²⁹ In all, the debilitating effects of

cyber espionage in the Philippines compromise national security. Its effects may be felt not only at the state level but may also transcend down to individuals.

Social Engineering: individual level

The Filipino public faces a multitude of challenges in cyberspace including social engineering, “a manipulation technique that exploits human error to gain private information, access, or valuables.”³⁰ Two elements are key in its operations – network vulnerability and human interaction. If the network is insecure, attackers can easily infiltrate it and compromise all the information of users connected to it. In a similar manner, if individuals are not careful and couldn’t identify which transaction is legitimate or not, there lies an issue of human error. The human aspect will be noted in this section.

Human nature dictates that when faced with a crisis, individuals express various emotions. This is largely the reason why many people get scammed. This was observed during the height of the COVID-19 pandemic when people were highly susceptible to fake information and cyber attacks. The most popular social engineering technique is phishing or the act of stealing important data or financial information through email.³¹ In 2022, the Philippines was reported as one of the top phishing email targets in Southeast Asia because of the boom of e-commerce platforms in the country.³² Meanwhile, smishing is a variant of phishing which involves similar activities but is done through text messages. Over the years, smishing has become more alarming in the Philippines, which led to the enactment of the Sim Card Registration Act of 2022 to counter smishing and easily identify attackers through attribution. Large telecom companies PLDT and Globe reported that they blocked more than a billion spam and malicious texts in less than a year.³³

The influx of social engineering techniques successfully targeting Filipinos present the need to look into the individual level further.

A survey reported that Filipinos rank second in the world in terms of time spent online, with an average of 10 hours and 27 minutes per day.³⁴ If social engineering continues, the vulnerability of Filipinos will heighten thereby becoming more insecure in cyberspace.

POLICY RECOMMENDATIONS

The discussion above has argued that cyber conflict, cyber espionage, and social engineering affect the Philippines in international, national, and individual levels, respectively. In consideration of these challenges, policy options and recommendations are necessary in moving towards the formulation of a cyber defense strategy.

Formulate a cyber defense strategy through consultations

This policy brief has provided multiple arguments for the formulation of a cyber defense strategy in the Philippines. In pursuit of this recommendation, the DND may conduct focus group discussions or consultations with various sectors in all levels – local government units, civil society organizations, cybersecurity companies, other government agencies, and the academe. It is important to note that to be able to effectively defend the whole nation, the formulation of a cyber defense strategy should go beyond the defense and military perspective.

The country’s cyber defense strategy may encapsulate approaches towards specific ends and concrete courses of action to achieve them. In this regard, investment on people and cyber defense infrastructure must be prioritized. The cases of cyber attacks in the country pointed out the importance of having efficient infrastructure, both hardware and software, and competent people operating these infrastructures. For the former, partnerships with cybersecurity companies and other government agencies are necessary in exchanging ideas and determining best practices. For the latter, it is

beneficial to involve technocrats and capacitate future cybersecurity professionals through education and training.

Although challenges will always be present, the country will benefit greatly from this initiative. At the international level, the country will gain more credibility in engaging with partners on joint cyber defense activities. It can also contribute more effectively in regional cybersecurity dialogues such as those conducted by the Association of Southeast Asian Nations (ASEAN) through the ASEAN Defence Ministers' Meeting (ADMM), the ADMM-Plus, and the ASEAN Experts' Working Group (EWG) on Cybersecurity, among others. At the national level, the publication of a strategy document will enable the cyber defense industry to flourish, thereby increasing opportunities for cybersecurity professionals, IT experts, and researchers. With a cyber defense strategy, cyber attacks like the ones perpetrated by APT groups can be prevented, minimizing the Philippines' vulnerability in cyberspace and maximizing the gains of technological advancement.

Ensure the integration of cybersecurity in digital transformation programs

As discussed above, the eGov SuperApp is a success by the government for the Filipinos. Indeed, the app may improve the way the public views government institutions in the country. In this regard, the inclusion of cybersecurity as one of the main considerations in the app's operations is vital. Adopting cybersecurity measures to secure personal information and economic transactions in the app is one way to increase public support and usage. This recommendation does not only apply to the eGov SuperApp but also to all digital transformation programs. It is important to note that digital transformation must proceed alongside cybersecurity and cyber defense. Negative repercussions may be expected if cybersecurity and cyber defense will remain in the periphery while the country's ICT capabilities are pursued separately.

Consider and invest in multi-level opportunities for cyber defense

In consideration of the multi-level challenges discussed in this policy brief, it is recommended for the government to consider and invest in multi-level opportunities for cyber defense. This includes cyber diplomacy, cyber resiliency, and cyber cognition.

a. Cyber diplomacy

At the international level, the Philippines may strengthen its bilateral relations with South Korea and Japan and enhance its alliance with the U.S. through cyber diplomacy. As South Korea is the first country in Asia to join the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence (CCDCOE) which comprises the world's leading experts on cyber defense, the Philippines may use this opportunity to engage with South Korea more to develop its own expertise.³⁵ This may be supported by both countries' close relations with the US and the US commitment to expand the scope of its engagement with both countries on cyber and space.³⁶ Meanwhile, the Philippines may also enhance cyber diplomacy with Japan specifically on cyber defense. At present, Japan aims to expand its cyber defense forces and advance the active cyber defense strategy.³⁷ Alongside the plans to acquire drones from Japan, the Philippines will benefit from Japan's expansion as it pursues its military modernization program and develops its cyber defense capability.³⁸

Meanwhile, in April 2023, the Philippines and the U.S. engaged in the Balikatan exercises which included the first iteration of the Cyber Defense Exercise (CYDEX) among military officers. The CYDEX benefits the Philippines in terms of enhancing people's expertise and addressing challenges in cyberspace. Moreover, the country recognizes the

need for the military to be ready and capable with the changing character of warfare.³⁹ The inaugural CYDEX is an indication of the commitment to enhancing the collective capabilities of the two allies.⁴⁰ Further, at the start of May 2023, the Bilateral Defense Guidelines was established which identified the improvement of cyber defense and cybersecurity cooperation as one of the courses of action to modernize the alliance.⁴¹

Aside from bilateral relations, the Philippines may contribute more effectively to the development and observance of cyber norms, which is a part of the entire United Nations framework of responsible state behavior in cyberspace.⁴² This may be pursued through the country's influence and power to engage with others in achieving favorable results.⁴³ According to the 2023 Lowy Institute Asia Power Index, the Philippines ranked the highest on defence networks among all indicators of power. Under this category is regional defence diplomacy, regional alliance networks, and global defence partnerships. The country's score on diplomatic influence also increased.

b. Cyber resiliency

At the national level, cyber resiliency must be promoted. Defined as the ability "to prevent, withstand and recover from cybersecurity incidents",⁴⁴ cyber resiliency is a sign of security, defense capability, and awareness. To be resilient is to be able to manage cyber attacks so that they don't compromise the country's national interests. Although attached to cybersecurity, cyber resiliency is different in the sense that it does not only involve the protection of cyberspace but also the ability to recover from and manage cyber attacks. Cyber resiliency is not achieved instantly. It is built on consistent commitment and efforts by all sectors of society to pursue cybersecurity.

In the Philippines, many news articles and pronouncements point to cyber resiliency as the cybersecurity goal of the country. On the part of the private sector, both Kaspersky and Microsoft expressed the need for the country to enhance its internal and external efforts towards cyber resiliency. Kaspersky suggested strengthening public and private partnerships and regional and international engagements, citing the 432.75% increase in cyber threats from 2017 to 2021.⁴⁵ Relatedly, Microsoft noted that pursuing cyber resiliency is the best way forward for the Philippines "to minimize risks and losses."⁴⁶ For the government, former DND Officer-in-Charge Senior Undersecretary Jose C Faustino Jr noted that cyber resiliency can be achieved "by proactively addressing emerging cyber threats, as well as scaling up and optimizing the use of information and communication technology."⁴⁷ In all, resiliency should be a key aspect of cyber defense.

c. Cyber cognition

At the individual level, greater attention to cyber cognition may aid the country. Cyber attacks are conducted to instill fear, anxiety, and terror in the public. This effect cannot be measured quantitatively yet holds equal value as the effects of physical violence.⁴⁸ With this, it can be argued that in crisis situations, individuals tend to be more susceptible to cyber attacks by prioritizing emotions over cognition. Cyber criminals use the intensity of these emotions to leverage their operations and manipulate vulnerable individuals.⁴⁹

In the Philippines, this can be addressed through cyber cognition which may be done through information drives, seminars, immersive activities, educational tours, and robust social media engagements. Initiatives for cyber cognition led by the DICT must be enhanced to cater to the fast-changing cyber threat landscape and to highlight

cyber defense more. It is important for Filipinos to be equipped with the ability to think clearly, understand information, and analyze them among other available information. This allows individuals to practice caution to prevent being subjected to attacks and avoid the tendency for cognitive heuristics or mental shortcuts that generate ill-conceived conclusions. Here, the accuracy of information must be ensured given that the cognitive process may be tampered with false information.⁵⁰

CONCLUSION

This policy brief provided a multi-level analysis on how a cyber defense strategy may be formulated in the Philippines. Cybersecurity challenges were also presented with international, national, and individual perspectives. First, cyber conflict between great powers confronts the international arena, which inevitably spills over to the Philippines and the way it pursues cyber defense. Second, cyber espionage plagues the country which not only affects public and private networks but ultimately, national interests. Third, social engineering targets Filipinos who prioritize emotions and are susceptible to false information. The confluence of these challenges and the ever-evolving nature of cyberspace prompt the Philippines to take necessary steps towards the protection of the cyber domain. Further, the challenges and corresponding policy recommendations discussed are a starting point from which a whole-of-nation approach towards a cyber defense strategy can be developed.

This month marks the first year in office of President Ferdinand Marcos Jr. This generates vast opportunities to boost the country's cyber defense capabilities. So far, only programs on digital transformation have been highlighted, especially as the country also celebrates the National ICT Month. On cyber defense, much is left to be done. If the current administration moves forward in the

right direction and publishes a cyber defense strategy, it will be the first document of its kind in the country. Indeed, this is instrumental not only for the DND but also for the entire nation. What the Philippines can and will do now certainly impacts how the country progresses into a more complex and competitive future.

ENDNOTES

¹ In this context, equalizer means the factor which makes all states equal, regardless of capabilities and economic wealth.

² Brigitte Dekker, Karthik Nachiappan, and Maaïke Okano-Heijmans, "Fostering digital connectivity in and with the Indo-Pacific: Opportunities for the European Union," *The Netherlands Institute of International Relations 'Clingendael'* (2021), 10. [https://www.clingendael.org/sites/default/files/2021-04/Report Digital Connectivity IndoPacific April 2021.pdf](https://www.clingendael.org/sites/default/files/2021-04/Report%20Digital%20Connectivity%20IndoPacific%20April%202021.pdf).

³ BBC, The Lazarus heist: How North Korea almost pulled off a billion-dollar hack, June 21, 2021, <https://www.bbc.com/news/stories-57520169>.

⁴ John Chalmers and Karen Lema, "For bank heist hackers, the Philippines was a handy black hole," *Reuters*, March 21, 2016, <https://www.reuters.com/article/us-usa-fed-bangladesh-philippines-idUSKCN0WM13B>.

⁵ Kaspersky, "Naikon Targeted Attacks," <https://www.kaspersky.com/resource-center/threats/naikon-targeted-attacks>.

⁶ 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/>.

⁷ Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1 (2012): 19 & 27-29, <https://doi.org/10.1080/01402390.2011.608939>.

⁸ Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies*; Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html.

⁹ Gelo Gonzales, "Ransomware attacks cost PH firms P40 million on the average in 2020," *Rappler*, May 26, 2021, <https://www.rappler.com/technology/ransomware-attacks-average-cost-philippines-firms-2020/>.

¹⁰ Secure Connections and The Asia Foundation, *Cybersecurity in the Philippines: Global Context and Local Challenges*, March 2022, Foreword. <https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf>.

¹¹ Philippine News Agency, "PH 4th among countries most targeted by web threats," February 21, 2022, <https://www.pna.gov.ph/articles/1168257>.

¹² Muhammad Zulhusni, "How important is AI to the fintech industry in the Philippines?" *Tech Wire Asia*, August 3, 2022, <https://techwireasia.com/2022/08/how-important-is-ai-to-the-fintech-industry-in-the-philippines/>.

¹³ Center for Research and Communication, "Delve Into the Philippine Market's Fintech Industry Via CRC's Consultancy Service Offerings for Investors," July 26, 2022, <https://crc.uap.asia/2022/07/26/delve-into-the-philippine-markets-fintech-industry-via-crcs-consultancy-service-offerings-for-investors/>.

¹⁴ International Trade Administration, "Philippines - Country Commercial Guide," July 25, 2022,

<https://www.trade.gov/country-commercial-guides/philippines-ecommerce#:~:text=Overview,Market%20Overview,with%2017%25%20growth%20through%202025>.

¹⁵ Daphne Galvez, "Gov't launches e-Gov Super App to enhance services, processes, combat corruption," *Philippine Daily Inquirer*, June 2, 2023, <https://newsinfo.inquirer.net/1778644/fwd-govt-launches-e-gov-super-app-bongbong-marcos-says-this-will-combat-corruption>.

¹⁶ eGOV PH, <https://e.gov.ph/>.

¹⁷ CNN Philippines Staff, "PH launches 'super app' for govt transactions," *CNN Philippines*, June 2, 2023, <https://www.cnnphilippines.com/news/2023/6/2/eGOV-PH-Super-App-launch-.html>; PTV News CF, "PH launches single govt portal 'eGov Super App'," *PTV News*, June 2, 2023, <https://ptvnews.ph/ph-launches-single-govt-portal-egov-super-app/>.

¹⁸ CNN Philippines Staff, "PH launches 'super app' for govt transactions."

¹⁹ Miguel Alberto Gomez, "The Challenge: Cyberspace and Security in the Indo-Pacific," *FACTS Asia*, October 24, 2022, <https://www.factsasia.org/blog/the-challenge-cyberspace-and-security-in-the-Indo-pacific/>; Tim Starks, "The U.S. lags on happiness, health, but it tops the list for cyber power," *The Washington Post*, September 27, 2022, <https://www.washingtonpost.com/politics/2022/09/27/us-lags-happiness-health-it-tops-list-cyber-power/>.

²⁰ Observer Research Foundation, "The Future of Cyber Warfare in the Indo-Pacific," no. 604 (2023): 6,8-9, https://www.orfonline.org/wp-content/uploads/2023/01/ORF_IB-604_Future-of-Cyber-Warfare-in-the-Indo-Pacific.pdf.

²¹ U.S. Embassy in Manila, "Fact Sheet: U.S.-Philippines Defense and Security Partnership," February 11, 2022, <https://ph.usembassy.gov/fact-sheet-u-s-philippines-defense-and-security-partnership/>.

²² Gregory B. Poling, "The Transformation of the U.S.-Philippines Alliance," *Center for Strategic and International Studies*, February 2, 2023, <https://www.csis.org/analysis/transformation-us-philippines-alliance>; Tarra Quismundo, "PH, US agree on 5 'bases'," *Philippine Daily Inquirer*, March 20, 2016, <https://globalnation.inquirer.net/137945/ph-us-agree-on-5-bases>.

²³ Global Times, "China-Philippines bilateral trade up 8.3% in first 11 months of 2022:MOFCOM," January 6, 2023, <https://www.globaltimes.cn/page/202301/1283346.shtml#:~:text=At%20the%20end%20of%202021,said%20at%20a%20press%20conference>.

²⁴ Agathe Demarais, "How the U.S.-Chinese Technology War Is Changing the World," *Foreign Policy*, November 19, 2022, https://foreignpolicy.com/2022/11/19/demarais-backfire-sanctions-us-china-technology-war-semiconductors-export-controls-biden/?tpcc=fp_live.

²⁵ Department of Information and Communications Technology. National Cybersecurity Plan 2022.

²⁶ Francis Domingo, "Strategic Considerations for Philippine Cyber Security," *Stratbase ADR Institute*, (2016): 7. DOI:10.13140/RG.2.1.4636.7768.

²⁷ Chris Bing, "A stolen Trump-Duterte transcript appears to be just one part of a larger hacking story," *CyberScoop*, May 31, 2017, <https://cyberscoop.com/apt->

[32-trump-duterte-hacking-xi-jinping-vietnam/](#); Miguel Alberto Gomez and Brandon Valeriano, "Frustrated with the Philippines, Vietnam Resorts to Cyber Espionage," *Council on Foreign Relations*, June 8, 2017, <https://www.cfr.org/blog/frustrated-philippines-vietnam-resorts-cyber-espionage>.

²⁸ Sarah Zheng and Jamie Tarabay, "Suspected State Hackers Stole Military Data from Asian Countries," *Bloomberg*, January 11, 2023, <https://www.bloomberg.com/news/articles/2023-01-11/suspected-state-hackers-stole-military-data-from-asian-countries#xj4y7vzkg>.

²⁹ Mark Bryan Manantan, "What the Huawei espionage controversy means to the Philippines," *Coral Bell School of Asia Pacific Affairs – Australian National University College of Asia & the Pacific*, March 25, 2019, <https://bellschool.anu.edu.au/news-events/news/6782/what-huawei-espionage-controversy-means-philippines>.

³⁰ Kaspersky, "What is Social Engineering?", <https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering>.

³¹ Christine Lisette Castillo, "Cyberspace as the New Domain for Great Power Competition: Strengthening the Philippines' Capability in a Complex Security Environment," *NDCP Executive Policy Brief*, June 26, 2020, 2-3, https://ndcp.edu.ph/wp-content/uploads/2022/01/EPB_2020-02_Castillo.pdf.

³² Tyrone Jasper C. Piad, "PH among top phishing email targets in Southeast Asia," *Philippine Daily Inquirer*, October 25, 2020, <https://newsinfo.inquirer.net/1684467/ph-among-top-phishing-email-targets-in-Southeast-asia>.

³³ Piad, "PH among top phishing email targets in Southeast Asia," *Philippine Daily Inquirer*; Reuters, "Philippine senate probes large-scale phishing scams," September 8, 2022, <https://www.reuters.com/world/asia-pacific/philippine-senate-probes-large-scale-phishing-scams-2022-09-08/>.

³⁴ Cristina Eloisa Baclig, "Social media, internet craze keep PH on top 2 of world list," *Philippine Daily Inquirer*, April 29, 2022, <https://newsinfo.inquirer.net/1589845/social-media-internet-craze-keep-ph-on-top-2-of-world-list>.

³⁵ Philippine News Agency, "SoKor becomes 1st Asian nation to join NATO's cyber group," May 5, 2022, <https://www.pna.gov.ph/articles/1173770>.

³⁶ Jim Garamone, "Austin Looks to Build on Strengths of Alliances With South Korea, the Philippines," *U.S. Department of Defense*, January 29, 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3281373/austin-looks-to-build-on-strengths-of-alliances-with-south-korea-the-philippines/>.

³⁷ Mao Kawano, "Japan to quadruple cyber defense forces, meeting threats head-on," *Nikkei Asi*, January 5, 2023, <https://asia.nikkei.com/Politics/Japan-to-quadruple-cyber-defense-forces-meeting-threats-head-on>.

³⁸ 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/>.

³⁹ Vince Ferreras, "PH seeks better cyber defense capabilities in Balikatan exercises," *CNN Philippines*, April 11, 2023, <http://www.cnnphilippines.com/news/2023/4/11/PH-cyber-defense-Balikatan-exercises-.html>.

⁴⁰ Indo-Pacific Defense Forum, "Inaugural cyber defense drill builds partnerships, capabilities at Balikatan," May 16, 2023, <https://ipdefenseforum.com/2023/05/inaugural-cyber-defense-drill-builds-partnerships-capabilities-at-balikatan/>.

⁴¹ The United States and the Republic of the Philippines Bilateral Defense Guidelines, <https://media.defense.gov/2023/May/03/2003214357/-1/-1/0/THE-UNITED-STATES-AND-THE-REPUBLIC-OF-THE-PHILIPPINES-BILATERAL-DEFENSE-GUIDELINES.PDF>.

⁴² Australian Strategic Policy Institute (2020, March). "The UN norms of responsible state behaviour in cyberspace," March 2020, 17, <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>.

⁴³ Lowy Institute Asia Power Index 2023 Edition, "Philippines," <https://power.lowyinstitute.org/countries/philippines/>.

⁴⁴ IBM, "What is cyber resilience?" <https://www.ibm.com/topics/cyber-resilience>.

⁴⁵ Arjay L. Balinbin, "Philippines must work with neighbors to build cyber resiliency – Kaspersky," *Business World*, July 7, 2022, <https://www.bworldonline.com/technology/2022/07/07/459598/philippines-must-work-with-neighbors-to-build-cyber-resiliency-kaspersky/>.

⁴⁶ Janvic Mateo, "Philippines urged to strengthen cybersecurity infrastructure," *Philippine Star*, November 28, 2022, <https://www.philstar.com/headlines/2022/11/28/2226952/philippines-urged-strengthen-Cybersecurity-infrastructure>; Microsoft Philippines Communications Team, "Microsoft defines digital threat landscape, advocates for stronger defense and resiliency in the Philippines," November 25, 2022, <https://news.microsoft.com/en-ph/2022/11/25/microsoft-defines-digital-threat-landscape-advocates-for-stronger-defense-and-resiliency-in-the-philippines/>.

⁴⁷ Priam Nepomuceno, "DND eyes to make PH more cyber resilient," *Philippine News Agency*, November 15, 2022, <https://www.pna.gov.ph/articles/1188583>.

⁴⁸ Ryan Shandler, Michael L Gross, and Daphna Canetti, "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis," *Journal of Global Security Studies* 8, no. 1 (2023): 4-5,15. <https://doi.org/10.1093/jogss/ogac042>.

⁴⁹ Castillo, "Cyberspace as the New Domain for Great Power Competition: Strengthening the Philippines' Capability in a Complex Security Environment," 2-3.

⁵⁰ Miguel Alberto Gomez and Eula Bianca Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats," *Politics and Governance* 6, no. 2 (2018): 61-63. <https://www.cogitatiopress.com/politicsandgovernance/article/view/1279>.

NDCP Executive Policy Brief

The Executive Policy Brief (EPB) is a publication series on national defense and security issues by the Research and Special Studies Division (RSSD) 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 the NDCP. The readers are free to reproduce copies mechanically, or to quote any part provided proper citations are made.

Copyright © National Defense College of the Philippines (NDCP) 2023. All rights reserved.

Author

Christine Lisette M. Castillo is a Defense Research Officer II in the Research and Special Studies Division of NDCP. Ms Castillo's research interests include cybersecurity, cyber defense, regional and international security cooperation, and women, peace, and security (WPS). For comments on the policy brief and other related engagements, please email christine.castillo@ndcp.edu.ph.

NDCP Editorial Board

LtGen Ferdinand M Cartujano PAF (Ret)
President

Capt Aldrin C Cuña PN (Res), MNSA
Executive Vice President

Mr Manmar C Francisco
Acting Chief, Research and Special Studies Division

Ms Arielle Ann Nicole Lopez
Senior Defense Research Officer



Please scan the QR code to access our Feedback Form for your comments, opinions, and suggestions. Thank you very much and we look forward to hear from you.

www.ndcp.edu.ph