EPB ISSN 2945-4689

National Defense College of the Philippines

EXECUTIVE POLICY BRIEF

Issue Number 2022-03

28 June 2022

Philippine Cybersecurity in Retrospect (2016-2021)

Christine Lisette M Castillo

Key Points and Policy Recommendations

- Develop cyber defense as a strategic capability. The Philippines' situation as a hotspot for cybercrime prompts the country to focus greater on cyber defense to safeguard vital networks and systems.
- Prioritize key cybersecurity concerns such as those involving cyber espionage, cyber terrorism, and cyber conflict.
- Promote personal cybersecurity. Individuals have the capacity to deter a cyber attack if they understand the measures they can undertake.

Cyberspace is a borderless domain that has moved from peripheral discussions to one of the core security concerns of various countries around the world. Unlike those in the physical domain, threats in cyberspace pose a different challenge for governments due to their uncertainty, complexity, and speed. In recent years, cyber criminals have increased their number and improved their skills as minimal resources are needed to be able to incur damage. As globalization only intensifies, the path towards the digitalization of all services becomes inevitable, thus furthering innovation but also creating more ground for cyber threat actors to operate. This perennial challenge remains to be a major concern in cyberspace. Key actors in cybersecurity, then, are faced with harnessing the full potential of cyberspace while mitigating the consequences of technological development.

No entity in the world can be spared from cyber threats in that anyone that is connected to the World Wide Web (WWW) is a potential victim of cybercrime. Even the most developed states, including cyber powers, still deal with cyber threats everyday. However, this situation is greater experienced by less capable states who struggle to address multiple security challenges while also trying to prioritize their cybersecurity agenda. The Philippines, for instance, is faced with difficulty managing the social and economic effects of cyber attacks on public and private networks in the country. This situation was heightened at the start of the COVID-19 pandemic in 2020 when everyone was compelled to conduct all activities online. Cognizant of these, it is important to assess the Philippines' cybersecurity posture for the past six years. While cybersecurity in the country existed prior to 2016, a more recent focus enables a well-informed and efficient approach to cybersecurity.

This policy brief aims to contribute to cybersecurity literature by exploring key issues and concerns that are relevant in a review. It will argue that the cybersecurity posture of the country has progressed not only because of the accomplishments but also the challenges in the past six years. Ultimately, points for consideration and policy recommendations will serve as bases for approaching cybersecurity hereon. In particular, this policy brief seeks to answer the following questions:

NDCP Executive Policy Brief (EPB)

A Publication Series on National 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.

1. How has cybersecurity in the Philippines progressed over the past six years (2016-2021)? Was cybersecurity a priority in key documents?;

2. What are the core cybersecurity challenges that hinder the Philippines in achieving cybersecurity? What do these challenges project to the country's cybersecurity posture?

3. Based on the country's progress and challenges on cybersecurity, what are the key points and policy recommendations that the new Philippine leadership[1] may consider moving forward?

In this pursuit, it is imperative to discuss the progress and challenges of the Philippines in managing cyber threats while also beefing up its cybersecurity capabilities for the past six years.

The Philippines' Cybersecurity Posture (2016-2021)

The Philippines' National Cybersecurity Plan 2022 defines cybersecurity as "the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets."[2] This definition signifies the country's commitment to employ all appropriate measures to protect cyberspace, a domain that has become paramount to Filipinos' ways of life.

In this pursuit, substantive progress on cybersecurity in the country has been noted over the years. As law enforcement is key in national development, several legislations have been created to safeguard information in networks and systems as well as to protect end users. First on the list is the Electronic Commerce Act of 2000 or Republic Act 8792, which recognized the digitalization of services at a time when information and communications technology (ICT) became more prominent in national economic development.[3] Second, the Anti-Photo and Video Voyeurism Act of 2009 or Republic Act No. 9995 penalizes persons who spread private photos or videos of someone on the Internet without the latter's written consent.[4] Third, the Anti-Child Pornography Act of 2009 or Republic Act No. 9775 gives value to children and the youth by safeguarding them against malicious, abusive, and obscene acts such as pornography.[5] Fourth, the Data Privacy Act of 2012 or Republic Act No. 10173 established the Data Privacy Commission which is tasked to oversee all functions related to securing personal information and facilitating a free flow of communication in government and private sectors.[6] Finally, the Cybercrime Prevention Act (CPA) of 2012 or Republic Act 10175 penalizes cyber criminals who engage in the misuse and abuse of all ICT devices, including illegal access to information therein and all activities done on and through the Internet for malicious and unjustified reasons.[7] The CPA was created to prevent and address the adverse effects of technological advancement.[8]

Given that Philippine cyberspace is vulnerable to all kinds of cyber threats, cybercrime laws such as the CPA are vital towards securing both cyberspace and its users. Indeed, according to the United Nations Office on Drugs and Crime (UNODC), "cybercrime law identifies standards of acceptable behaviour for ICT users" which regulates cyber activities and enables easier attainment of cyber justice.[9] The aforementioned legislations, especially the CPA, served as pillars in advancing Philippine cybersecurity from 2016 to 2021. In the past six years, cybersecurity progress can be categorized into three (3) areas.

***International Cooperation*.** The accession of the Philippines to the Budapest Convention on Cybercrime in 2018 signaled the growing necessity to be a part of an international collaboration that is dedicated to combating cybercrimes.[10]

To note, the Convention was drafted in 2001 after the Council of Europe and four other countries[11] recognized the global nature of cybercrime and the relative necessity to create an international treaty as a response.[12] It was also brought by the bureaucratic process of acquiring digital evidence across borders, hindering efficient data gathering and ultimately, the achievement of justice.[13] With this, the Convention aims to harmonize national policies on cybercrime, increase cooperation among nations, and support investigations for the prosecution of cyber criminals.[14] Some of the crimes included in the Convention are computer-related fraud, misuse of devices, and child pornography.[15]

According to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCE), “More than 80% of world states have based their domestic legislation on cybercrime” in the Convention.[16] This includes the Philippines as proven by the CPA. Cognizant of the fact that cybercrimes are not an individual actor’s sole undertaking, the Philippines’ accession to the Convention did not only reinforce the importance of cybersecurity for the country but also gave greater opportunity for the Philippines to engage with other Parties under the ambit of a common criminal policy.[17] Should a cybercrime occur, the Convention allows the country to seek assistance from others in the detection, investigation, and prosecution processes. Also, as the first country in Southeast Asia to become a Party to the Convention, the country has become a catalyst for the rest of the region to follow suit.[18] In Southeast Asia, the Association of Southeast Asian Nations (ASEAN) remains to be the main platform for cross-border collaboration. The Philippines is an active contributor in ASEAN’s cybersecurity plans and programs such as the ASEAN ICT Master Plan 2020, Master Plan on ASEAN Connectivity 2025, and the ADMM-Plus Experts Working Group on Cybersecurity, among others.[19] With this, and with the Philippines being a Party to the Budapest Convention, more opportunities for cybersecurity will be harnessed which can then be applied on domestic initiatives.

***Government Institution*.** The establishment of the Department of Information and Communications Technology (DICT) in 2016 is a monumental step towards the long-term goal of a secure and technologically-capable Philippines. As stipulated in Republic Act 10844, the DICT is tasked to be the lead government agency in the planning, development, and promotion of the national ICT development agenda.[20] As a background, efforts to establish the DICT have long started to advance. In 2004, former President Gloria Arroyo signed Executive Order 269 which established the Commission on Information and Communications Technology (CICT). Several years later, in 2011, the late President Noynoy Aquino issued Executive Order 67, reorganizing the CICT to the Information and Communications Technology Office (ICTO) under the Department of Science and Technology (DOST). However, even with these initiatives, the desire to pursue the establishment of a department still continued. This was exemplified by the bills in Congress that were filed since 2004.[21] At present, cybersecurity matters are mostly managed by the Cybersecurity Bureau under the DICT and the Cybercrime Investigation and Coordinating Center (CICC) which is an attached agency of the DICT.

From initially putting low priority on cybersecurity[22] to having established an institution which puts cybersecurity as a key priority, this remarkable reconsideration of the government has been brought both by the regional environment and public perception. In the region, two ASEAN member states have established national agencies prior – Malaysia in 2007 with CyberSecurity Malaysia, and Singapore in 2015 with the Cyber Security Agency of Singapore.[23] It was an opportunity for the Philippines to follow the same path and contribute to the region’s progress in cyberspace. In the country, it was a time of a government transition. As the RA 10844 was signed a month before a new administration took over, it was in the interest and benefit of the administration of the late President Noynoy Aquino to leave office with a legacy. This has contributed significantly to public perception at the twilight of his administration. Moreover, by putting the establishment of DICT as one of the five priority reform measures in his administration, President Noynoy Aquino set the direction towards the country's cybersecurity goals, from which the succeeding administration of former President Rodrigo Duterte was able to continue.[24] As stipulated by law, the DICT, particularly the CICC, is responsible for the creation of a national plan that will reflect the government's goals and programs for cybersecurity.

Plans and Programs. On *plans*, the Philippines' National Cybersecurity Plan (NCSP) 2022 which was released in 2017 serves as the main document for the pursuit and development of cybersecurity in the country. The NCSP outlined four primary goals: making critical information infrastructure (CII) trusted and secure; making government information environment secure; making businesses secure; and making individuals aware and secure.[25] In terms of setting the agenda, these goals are a well-rounded representation of the country's desire for innovation and progress. Further, these goals cover the most important aspects of development - securing the systems where economic, social, and security matters are conducted, and protecting the people who are the users of cyberspace. As the country's first cybersecurity plan in history, the NCSP was able to effectively present the Philippines' stance and direction on cybersecurity. While it is not a strategy, the NCSP is a vital foundation from which programs and projects have been and are being built.

In relation to the NCSP, the government's National Security Policy (NSP) has incorporated cybersecurity as a point of discussion. In brief, the NSP 2011-2016 first mentioned cybercrime as a transnational crime of concern, as influenced by the then on-going and eventual passage of the CPA in 2012. According to the NSP 2011-2016, as reliance on cyberspace intensifies, the vulnerability of cyber attacks against its users increases. This statement was further reinforced and supplemented in the NSP 2017-2022, which included Informational and Cyber Security as one of the 12-point National Security Agenda of the government. The goal in relation to this is twofold: first, to safeguard state secrets from cyber espionage that will compromise national security interests; and second, to protect vital sectors such as the communications industry, and banking and financial institutions, among others from cyber attacks that will derail operations and cause deep economic and societal damage. Further, the NSP 2017-2022 indicated that as the Internet provides "speed, convenience, and anonymity," actors and their operations have evolved. From being executed by small groups and individuals, cybercrimes are now perpetrated by large networks, such as the Advanced Persistent Threat (APT) groups. Therefore, cybercrime operations have become highly organized and elusive. The NSP 2017-2022 offered two ways to address the challenge - by developing the country's cyber capabilities and by expanding the pool of cybersecurity professionals and experts.[26]

Another important document is the National Security Strategy (NSS) 2018 which mentioned the need to "provide strong cyber infrastructure and cybersecurity" amidst cyber attacks.[27] The NSS recognized that cyberspace is being used in multiple ways - from research, education, and entertainment to spreading extremist propaganda and false information. As it was stated, "Our inability to harness the potentials and thwart the threats from cyberspace could imperil the country's vital interests, critical infrastructure and installations, institutions, and the patrimony of the country and the people."[28] With this, the government, through the NSS, set forth a blueprint for strategic action to assess the country's vulnerabilities in cyberspace.[29] In relation to the NSS, the National Defense Strategy (NDS) 2018 stressed the importance of cybersecurity in defending the country from national security threats. The NDS identified the intensifying threat in cyberspace as a concern in the country's strategic environment.[30]

On *programs*, the DICT has the Computer Emergency Response Program which comprises national, government, and sectoral levels. Particularly, the National Computer Emergency Response Team (NCERT or CERT-PH) is "responsible for receiving, reviewing, and responding to computer security incident reports and activities." It consists of four sections: Security Operations Center Section; Digital Forensics Section; Incident Response Section; and Cyber Threat Monitoring and Information Sharing Section.[31] NCERT is instrumental in ensuring that cyber incidents are immediately addressed and that networks are regularly monitored and tested for vulnerabilities.

Moreover, the DICT launched its use of the CHIP strategic framework last year to "improve the Philippines' readiness for full and inclusive participation in the global digital economy and as a driver of digital transformation."[32] CHIP – which means Connect, Harness, Innovate, and Protect – is a framework which will accelerate the growth of the country after the pandemic brought economic downturn. Specifically, the Protect component aims to mitigate risks on cybersecurity and privacy as various sectors employ digital operations.[33]

Programs were also created in the field of education. In recent years, several universities in the country started to offer degree programs on cybersecurity. The AMA University is the first to offer the Bachelor of Science in Cybersecurity which was launched in 2016.[34] The same degree is also offered by the Holy Angel University with an addition of the first master's degree on cybersecurity in the country, the Professional Science Master's in Cybersecurity, which was offered in 2018.[35] Ateneo de Davao University also started to offer a Cybersecurity Track under its Bachelor of Science in Information Technology in 2019.[36] Aside from these degree programs, other courses have been created such as the Executive Diploma Program in Cybersecurity in the De La Salle College of Saint Benilde[37] and the Professional Course on Digital Governance and Cybersecurity in the University of the Philippines.[38] These programs and courses ought to augment the cybersecurity skills gap in the country which hinders the attainment of cybersecurity goals.

Public awareness programs were also pursued. The CICC Cyber Patrol Program educates the public by engaging them as partners against cybercrime. In this regard, the CICC conducts webinars, trainings, and campaigns across the country.[39] Awareness is also beneficial for small and medium-sized businesses (SMBs) who shifted to online platforms at the start of the pandemic. According to a 2021 study by information technology (IT) company Cisco, more than half of the surveyed businesses in the country suffered cyber attacks since the start of the pandemic. Aside from this, 70% believe that a cyber incident could end their businesses.[40] Indeed, this concern is warranted because NCERT reported that in 2021, it handled 1,174 cyber incidents, with malware and malicious files topping the list at 39.4%.[41]

These signify the need to boost initiatives on cybersecurity awareness. The Cybersecurity Awareness Month which is held every October and the National Cyber Drill held every November contribute in developing the understanding of the public on cybersecurity and their knowledge on responding to cyber threats, should they encounter one. In 2021, the National Cyber Drill aimed "on enhancing public awareness and assessing the public's perspective on cybersecurity and their capacity to protect themselves from cyber threats and cyber attacks."[42]

The progress that was discussed is significant. However, the Philippines is far from achieving a safe and secure cyberspace for all. Even with international collaboration, the establishment of a government institution, and the conduct of national plans and programs, challenges remain inevitable.

Challenges and Implications to Philippine National Security

Cybersecurity statistics and reports all indicate that the Philippines is a hotspot for cyber attacks. In banking, the Bankers Association of the Philippines (BAP) reported that P1 billion was lost in 2021 alone due to fraud and unauthorized withdrawals. Indeed, as exacerbated by the COVID-19 pandemic, financial services are among the most targeted by hackers.[43] Similarly, the Philippines ranked 4th globally as the country that was most targeted by web threats in 2021. Notably, cyber threats that were detected in the country from 2017 to 2021 have increased tremendously at 433 percent.[44] The cybersecurity challenges faced by the country continue to occur and proliferate because of the following points.

One challenge is that the Philippines tends to be merely reactive instead of proactive. This was exemplified first in 2000 when, after the highly controversial "I Love You" virus which was developed by a Filipino brought global economic damage, the Philippines passed the E-Commerce Law in an attempt to address the issue and prevent similar cybercrime in the future. However, said law, having been passed two months after the incident, cannot be applied retroactively.[45] With this, the perpetrator was freed without any charges. This incident revealed that the absence of a cybercrime law in the country has negative consequences.

More recently, in 2016, two major hacking incidents alarmed not only the Philippines but also the world. First, in February 2016, US$ 81 million from the account of the Bangladesh Bank in the Federal Reserve Bank in New York was illegally transferred to four fictitious accounts in the Rizal Commercial Banking Corporation (RCBC) in Makati City, Philippines.[46] Of the total amount, only US$ 16 million was recovered and the rest was laundered in casinos in Manila.[47] Second, in March of the same year, the hacker groups Anonymous Philippines and Lulzsec Pilipinas hacked into the website of the Commission on Elections (Comelec) and obtained confidential information of registered voters, a move that was carried out as a protest against the Comelec on the insecurity of the electoral system. In April, a few weeks before the national elections, the Comelec's voter database was leaked, exposing all private information of more than 55 million registered voters.[48] These two hacking incidents led the government to boost its efforts in full-scale, having passed RA 10844 or the establishment of the DICT in May of the same year.[49] Although a direct connection between the aforementioned cyber hacking incidents and the passage of the law was not stated, the former clearly influenced the latter and prompted the government to take action as a response.

Another challenge is the initial low prioritization given to ICT-related issues, especially cybersecurity. For instance, the passage of the law which established the DICT took more than a decade since the first bill was submitted to Congress.[50] During this time, there was a view that the DICT is not yet a necessity. Since it was a topic of contention then, a forum conducted in 2012 posed the question "DICT: Is It Really Necessary for Philippine Transformation?" Indeed, if the establishment of the DICT has long been discussed in Congress, which signals policymakers' belief in its necessity, why did its passage take so long? It was noted that sentiments on developing ICT capabilities of the country were divided at that time as many were still unsure of the role of the DICT, and since the government already has the ICTO. Put simply, the establishment of the DICT was not a priority.[51] It can be opined that the Department's eventual establishment was an action done because of the inevitable digitalization and the alarming rate by which cyber threats occur as years pass. Low prioritization of cybersecurity can also be observed in the passage of the CPA in 2012. With the "I Love You" virus having occurred in 2000, one would assume that a cybercrime law will be passed soon after. Contrary to this, and even with the cyber threats that were present years before the CPA's passage, it was not considered a policy priority. In comparison to other issues, the consequences of cybercrime might have been perceived as trivial then.

Third, while progress in connectivity and digital transformation is notable, cybersecurity does not fare at the same level. In 2018, Cisco released the Asia Pacific Security Capabilities Benchmark Study which noted that 51% of security alerts are not investigated in Philippine companies. This raises concern because a portion of this percentage might be legitimate threats to the companies.[52] In relation, a 2021 study by Cisco noted that 35% of the cybersecurity technologies used by Philippine companies are outdated.[53] These reports suggest that despite the leap in digital transformation since 2016,[54] many institutions still suffer from lack of capacity to manage cyber threats. This became more challenging as cyber threats continue to increase in number and effect, most especially since the start of the pandemic. These cyber incidents suggest that there is a disproportionate focus between cybersecurity and innovation. While digital transformation is indeed imperative, it is important to note that cybersecurity initiatives must not be disregarded. This is particularly beneficial for the country's cybersecurity maturity which, as pointed by DICT Acting Secretary Emmanuel Rey R. Caintic, is yet to improve from the infancy stage.[55]

The fourth challenge is also an issue of disproportionality. According to a 2021 report by Sophos, IT budgets in Asia Pacific and Japan remain stagnant despite a notable rise in cyber attacks.[56] To note, cyber attacks in the Philippines increased to 31% in 2021, compared to 24% in 2020. In this situation, having a low budget while cyber threats continue to proliferate will cause more cyber challenges. As pointed out by Trevor Clarke, lead analyst and director at Tech Research Asia, "Ultimately, security is about right-sizing the risk. If the risk increases, budgets should also increase. Yet, in this climate of uncertainty, we've seen organizations take a conservative approach to security spending, which is limiting their ability to stay ahead of cybercriminals." This situation stemmed from executive indifference or the downplay of cyber threats among decision-makers, which is a huge concern because they are the ones responsible for the cybersecurity of their respective companies. Another related disproportionality as opposed to the fast-paced increase of cyber attacks is the gap on cybersecurity professionals in the Philippines. In this manner, how can Philippine organizations manage to thwart cyber attacks if they lack enough cybersecurity skills and are faced with difficulty in recruiting them?[57]

Cybersecurity progress in the past six years has shown the country's commitment to securing the nation in a highly digital world. As the country is short-handed in human resource and capability, the roles of the government, private institutions, and the public are essential in pursuit of cybersecurity. With this, persisting challenges could be confronted and addressed successfully. In all, both the progress and challenges contributed to Philippine cybersecurity posture at present.

CYBERSECURITY CONSIDERATIONS

In the Philippines, cybersecurity has become a part of discussions on national security, military modernization, and economic development, among others. At present, cybersecurity does not solely affect cybersecurity professionals and IT experts but also the general public. As cyber threats affect everyone who use the Internet and ICT devices, cybersecurity has undeniably generated more concern, attention, and resources. For further discussion, the following cybersecurity considerations were noted.

First, it's difficult to consider the economic trajectory of the Philippines without regard for cybersecurity as it relies on economic growth for survival. Secure Connections, in its 2022 report, stressed that economic development and cybersecurity are "intimately related".[58] As the Philippine economy grows, technology also advances. On the one hand, cyberspace has opened opportunities for businesses to prosper and expand beyond a country's borders.[59] On the other hand, because of this dynamic, cyberspace also created risks for the economy in the form of cyber threats which incur economic costs. Indeed, according to a 2018 study by Frost & Sullivan, a market consulting and training company, cyber attacks can potentially cost the Philippines USD 3.5 billion or 1.1% of the country's total GDP.[60] Several fraud incidents involving banks in recent years have proved this.

Second, the digitalization of almost all day-to-day activities has inevitably drawn people to the understanding and awareness of cyberspace. For example, Filipinos rank second globally on spending the most time on the Internet, according to the Digital 2022 Global Overview Report released at the start of the year. In using social media for work, the Philippines also ranked second globally.[61] Further, data and statistics portal Statista recorded that the number of social media users in the country is continuously increasing at 81.53 million in 2021, and is predicted to continue to increase steadily.[62] One of the reasons why the Philippines has been placing among the top rankings consistently is because of the increased usage of e-commerce platforms which was heightened by the pandemic.[63] Notably, although this was the first time in seven years that the country did not get the top one ranking on Internet usage, the current ranking is still an indication that the Philippines becomes increasingly reliant on cyberspace.

This can be exemplified by the country's efforts to improve its Internet speed. As of writing, the Global Internet Speed Index by Ookla indicates that the country's average speed in mobile downloads is 19.45 Mbps (Megabits per second) while the average speed in fixed broadband downloads is 55.21 Mbps.[64] This is a huge leap from the average speed in 2016 which are 7.44 Mbps for mobile downloads and 7.92 Mbps for fixed broadband.[65] The number of places with free public WiFi has also increased from 2016 to present. As of October 2021, there are 11,203 free WiFi sites across the country, 4,305 of which were installed in 2020 alone, in comparison to the 800 yearly installations from 2016-2019.[66] Notably, the faster internet speed and increased free Wifi sites were carried out by the DICT through the 2017 National Broadband Plan and Republic Act 10929 or the Free Internet Access in Public Spaces Act of 2017, respectively. According to former DICT Secretary Gringo Honasan II, the DICT strives in one of its goals "to connect all Filipinos to the benefits of the digital economy," wherever in the country.[67]

Third, the effects of cyber threats range from small-scale to large-scale. From individuals, to agencies, to large organizations, and even the state, no entity is spared from the disruption caused by cyber attacks. This simple fact made cybersecurity even more relevant and necessary. This has also led the public to become more aware and more responsible in cyberspace, hence the emergence of cyber hygiene practices. Indeed, cybersecurity cannot be restricted as the responsibility of a single actor alone because everyone has valuable roles.

POLICY RECOMMENDATIONS

The role of the Department of National Defense (DND) in cybersecurity particularly lies in cyber defense. The NCSP noted the responsibilities of the DND in this regard: 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 cybercrimes under military jurisdiction.[68] Cognizant of the challenges and key points that were discussed, the following policy recommendations are relevant to the DND in the country's pursuit of cybersecurity.

First, develop cyber defense as a strategic capability. Contrary to earlier notions that cyber offense is better employed as a strategy than cyber defense, the latter is preferable for several reasons. Usually, militaries around the world prefer cyber offense because "It will be cheaper and easier to attack information systems than it will be to detect and defend against attacks."[69] Indeed, the attacker has the advantage by having the sole control of the time, date, and specifics of the cyber attack. Also, the attack is always executed when the defender least expects it. While this is technically correct, what was not explained is that the uncertainty of cyberspace gives an opportunity for the defender to expand its ways and adapt. Therefore, the defender can deter the intrusion at any given point during the cyber attack, rendering the attack a failure. In this case, the attacker loses to the defender, even after spending months or years trying to plan the attack and allocating resources for the operation.[70]

This has proven that a robust cyber defense is necessary for the Philippines. Although it is ideal that the country also possess a cyber offense capability, the Philippines' situation as a hotspot for cybercrime prompts the country to focus greater on cyber defense to safeguard vital networks and systems. Therefore, the DND may consider allocating viable financial and human resources to enhance its cyber defense. The Armed Forces of the Philippines (AFP) Cyber Defense Exercise (CYDEX) held annually is instrumental in developing the capability and competency of the AFP Cyber Defense Force".[71] In relation to the CYDEX, the Department may explore training White Hat Hackers (WHHs) to better equip the country's cyber defense. In all, these measures may be incorporated in a national cyber defense plan or strategy. The creation of this plan has been noted in the NDS but progress on this endeavor is yet to be determined.

Second, prioritize key cybersecurity concerns. The path towards cybersecurity is challenging, but prioritizing key concerns can generate meaningful progress, most especially that the Philippines faces a range of cyber threats. The key concerns that need to be prioritized are:

a. **Cyber espionage**. Cyber espionage is defined in the NCSP 2022 as "the use of computer networks to gain illicit access to confidential information, typically that by a government or other organization."[72] Several APT groups, which are considered the world's oldest, most skilled, and most active agents of cyber espionage,[73] target the Philippines to steal secrets and obtain geopolitical intelligence.[74] This, of course, is not only politically-inclined. Much of these cyber espionage operations are economically-motivated. For instance, China employs cyber espionage to achieve its goal of being the largest economy in the world.[75] This is relevant to the Philippines as it considers China as one of its security partners, as indicated in the NDS.

b. **Cyber terrorism**. On cyberterrorism, the main concern is to prevent the thriving recruitment of terrorist groups online. Part of the recruitment process is information operations, which the terrorists use to communicate to people internationally. Terrorist group, Al Qaeda, harnessed the power of the Internet after 9/11 when no country was a safe shelter for the group. Technological development allowed Osama Bin Laden, the group's leader, to deliver speeches in a hideout and upload the same online for public viewing. Recruitment starts when people who viewed the videos positively are targeted.[76] The Philippines, having a long-running counterterrorism campaign, must give more attention to cyber terrorism. Moreover, as the NSS identified ending internal armed conflicts, violent extremism, and terrorism as a top security concern, the monitoring of websites and social media accounts is important to combat cyber terrorism and be able to take down any sign of terrorist propaganda and brainwashing online. It is important to note that as technology advances, terrorists also adapt.

c. **Cyber conflict**. This will affect the Philippines because of competing cyber powers in the Asia-Pacific region such as the US, China, North Korea, South Korea, and Japan. The country may be trapped in a cyber conflict that it is not a part of in the first place. This becomes more complicated as cyber conflict can become a tool to advance foreign policy interests.[77]

By prioritizing these three concerns, not only that the issue of low prioritization on cybersecurity can be addressed but also the goals set by the government on digital transformation and greater connectivity will have more merit. Further, these concerns may be highlighted in the earlier recommended creation of a national cyber defense plan.

Third, promote personal cybersecurity. As previously discussed in the first policy recommendation, attackers or cyber criminals carefully plan their move, which can take years, before executing the actual series of attacks. In this situation, they can be deterred at any point during the attacks and fail, or they can succeed, but the likelihood of success can be limited through effective cyber defense measures. Individuals have the capacity to deter a cyber attack if they understand the measures they can undertake. In order to protect their devices and systems from cyber attacks, individuals should take note of the following measures: a) create a secure password; b) keep operating systems up-to-date; c) backup files; d) be cautious when using public WiFis; and e) beware of business email compromise (BEC).[78] The DND, through its Office for Cyber and Information System Management and the AFP Cyber Group, can expand its reach online and on the ground with information campaigns and cybersecurity tips for the public. In relation, the Department can maximize its platform and partner with non-government organizations during the Cybersecurity Awareness Month held every October annually.

CONCLUSION

At the dawn of the new Philippine administration, foreign policy priorities and national security interests are affirmed. While traditional security issues will continue to figure prominently in decision-making, non-traditional security issues have shaped the way the concept of security is perceived. Cybersecurity, in particular, has developed to be regarded as one of the most vital concerns of all actors from individuals to the state, due to the wide-ranging implications of cyber threats. In the Philippines, from 2016 to 2021, progress was seen in the country's accession to the Budapest Convention on Cybercrime, in the establishment of the DICT, and in the national plans and programs being implemented. But alongside these positive strides, the challenges such as the country's reactive tendency, low prioritization of cybersecurity, and disproportionate focus are also evident. Through a retrospective discussion of both the progress and challenges in cybersecurity as well as identifying key points thereafter, this policy brief has assessed the country's cybersecurity posture in the past six years. It is in the interest of the Philippines that the policy recommendations provided herein contribute significantly towards a resilient, mature, and secure cyberspace as the nation moves forward in an ever-evolving cyber threat landscape.

Christine Lisette Castillo, MIS *is a Defense Research Officer II at the Research and Special Studies Division (RSSD) of the National Defense College of the Philippines. For comments and suggestions, please email at christine.castillo@ndcp.edu.ph.*

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.

[1] On 30 June 2022, Ferdinand “Bongbong” Marcos Jr. will take his oath as the 17th President of the Republic of the Philippines.

[2] Department of Information and Communications Technology, *National Cybersecurity Plan 2022,* 46.

[3] Official Gazette, *Electronic Commerce Act of 2000*, June 14, 2000, https://www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792-s-2000/.

[4] The Lawphil Project, *Anti-Photo and Video Voyeurism Act of 2009*, July 27, 2009, https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html

[5] Other legislations related to this such as the Special Protection of Children Against Abuse, Exploitation, and Discrimination Act of 1992 or RA 7610, the Expanded Anti-Trafficking in Persons Act of 2012 or RA 10364, and the Anti-Violence Against Women and Children Act of 2004 or RA No. 9262, contain provisions that are intended to protect women and children online.

[6] National Privacy Commission, *Data Privacy Act of 2012,* July 25, 2011, https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf.

[7] Official Gazette, Cybercrime Prevention Act of 2012, July 25, 2011, https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf.

[8] Realisan Almeda Bernardino Rotao & Associates Law Offices, “The Cybercrime Law | What is the Purpose of RA 10175,” https://ralblaw.com/what-is-the-purpose-of-ra-10175/.

[9] United Nations Office on Drugs and Crime, “The role of cybercrime law,” https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

[10] Council of Europe, “Philippines,” April 23, 2020, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB#:~:text=The%20Philippines%20is%20a%20party,of%20a%20sound%20cybercrime%20legislation. https://legacy.senate.gov.ph/17th_congress/resolutions/resno89.pdf.

[11] COE members and Japan, US, South Africa, and Canada.

[12] “Convention on Cybercrime,” November 23, 2001, *European Treaty Series - No. 185*, https://rm.coe.int/1680081561.

[13] Council of Europe, “Towards a Protocol to the Budapest Convention,” September 5, 2019, https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.

[14] European Commission, “Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention,” February 5, 2019, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_865.

[15] Convention on Cybercrime, https://rm.coe.int/1680081561.

[16] Dominik Zachar, “Battling Cybercrime Through the New Additional Protocol to the Budapest Convention,” *NATO Cooperative Cyber Defence Centre of Excellence,* https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/.

[17] Convention on Cybercrime, https://rm.coe.int/1680081561.

[18] Keiko Kono, “ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone,” *NATO Cooperative Cyber Defence Centre of Excellence,* https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/.

[19] Christine Lisette M Castillo, “Pursuing Regional Cyber Cooperation: Implications for the Philippines and the ASEAN,” *NDCP Executive Policy Brief,* March 26, 2021, https://ndcp.edu.ph/wp-content/uploads/2022/01/New-EPB-Design_Castillo-1Q-EPB.pdf.

[20] Official Gazette, *Department of Information and Communications Technology Act of 2015,* July 27, 2015, https://www.officialgazette.gov.ph/2016/05/23/republic-act-no-10844/.

[21] Disini & Disini Law Office, “A Win for ICT: Towards a Department of Information and Communications Technology,” June 5, 2015, https://elegal.ph/a-win-for-ict-towards-a-department-of-information-and-communications-technology/.

[22] Helen P Macasaet, “DICT: Is it really necessary for PH transformation?” *Philippine Daily Inquirer,* August 6, 2012, https://business.inquirer.net/75193/dict-is-it-really-necessary-for-ph-transformation.

[23] AT Kearney, “Cybersecurity in ASEAN: An Urgent Call to Action, “ 2018, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34#:~:text=These%20include%20Singapore%20(Cyber%20Security,of%20Information%20and%20Communications%20Technology)%20.

[24] Disini & Disini Law Office, “A Win for ICT: Towards a Department of Information and Communications Technology.”

[25] Department of Information and Communications Technology, *National Cybersecurity Plan 2022,* 3, https://dict.gov.ph/wp-content/uploads/2019/07/NCSP2022-rev01Jul2019.pdf.

[26] National Cybersecurity Plan 2022, 16,17,25.

[27] National Security Council, *National Security Strategy 2018,* 65-66, https://nsc.gov.ph/images/NSS_NSP/NSS_2018.pdf.

[28] National Security Council, *National Security Strategy 2018,* 65.

[29] National Security Council, *National Security Strategy 2018,* 66.

[30] Department of National Defense, *National Defense Strategy 2018-2022,* 17, https://www.dnd.gov.ph/Files/ShowFile?url=/FilesUploaded/Ckeditor/file/NDS_7_August_2019.pdf.

[31] National Computer Emergency Response Team, “CERT-PH,” https://www.ncert.gov.ph/about-us/ncert/.

[32] Department of Information and Communications Technology, “DICT launches CHIP strategic framework to improve PH readiness for the global economy,” June 10, 2021, https://dict.gov.ph/dict-launches-chip-strategic-framework-to-improve-ph-readiness-for-the-global-digital-economy/.

[33] Department of Information and Communications Technology, *The DICT CHIP Implementation Plan,* https://dict.gov.ph/wp-content/uploads/2022/05/CHIP-Implementation-Plan-May-4-2022.pdf.

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

[35] Holy Angel University, “School of Computing,” https://www.hau.edu.ph/programs/school-of-computing/79.

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

[37] De La Salle College of Saint Benilde, “Cybersecurity,” https://www.benilde.edu.ph/continuing-education/space-cybersecurity/.

[38] UP Diliman Extension Programs in Pampanga and Olongapo, “Professional Course,” https://upepp.upd.edu.ph/academics/professional-course/.

[39] Cybercrime Investigation and Coordinating Center, “Cyber Patrol,” https://cicc.gov.ph/awareness-campaign/cyber-patrol/.

[40] Cisco Secure, “Cybersecurity for SMBs: Asia Pacific Businesses Prefare for Digital Defense,” September 2021, 6-8, https://www.cisco.com/c/dam/global/en_sg/products/security/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf.

[41] National Computer Emergency Response Team, “1174 Incidents Handled from January 1 to December 31, 2021,” https://www.ncert.gov.ph/page/2/?fbclid=IwAR1oKNBBkZ3TrsuuJWnyArrWaFa-He26SV9MKtcmNbgidEmyk6sSWKlutOY.

[42] National Computer Emergency Response Team, “National Cyber Drill 2021,” https://www.ncert.gov.ph/ncd2021/. CT Link, “Cybersecurity Awareness In The Philippines,” https://www.ctlink.com.ph/cybersecurity-awareness-philippines/.

[43] Bronte H Lacsamana, “Enterprise tech, financial services most vulnerable to cyber attacks - Secuna,” *Business World,* May 11, 2022, https://www.bworldonline.com/technology/2022/05/11/447702/enterprise-tech-financial-services-most-vulnerable-to-cyberattacks-secuna/.

[44] Philippine News Agency, “PH 4th among countries most targeted by web threats,” February 21, 2022, https://www.pna.gov.ph/articles/1168257#:~:text=MANILA%20%E2%80%93%20For%20the%20entire%202021,Kaspersky%20Security%20Network%20(KSN).

[45] LA Times Archive, “Philippine Law Not Applicable in ‘Love Bug’ Case, Official Rules,” *Los Angeles Times,* May 18, 2000, https://www.latimes.com/archives/la-xpm-2000-may-18-fi-31308-story.html. Stephen Lawson, “New e-commerce law won’t stop hackers: Philippine prosecutor,” *Computer World,* August 23, 2000, https://www.computerworld.com/article/2596633/new-e-commerce-law-won-t-stop-hackers--philippine-prosecutor.html.

[46] Nancy C Carvajal, Rex David Morales, and Angelica Carballo Pago, “What went before: The Bangladesh Bank Heist,” *Philippine Center for Investigative Journalism,”* September 21, 2020, https://pcij.org/article/4291/what-went-before-the-bangladesh-bank-heist.

[47] Geoff White, “The Lazarus heist: How North Korea almost pulled off a billion-dollar hack,” *BBC News,* June 21, 2021, https://www.bbc.com/news/stories-57520169

[48] Philippine Daily Inquirer, “IN THE KNOW: The 2016 ‘Comeleak’,” January 12, 2022, https://newsinfo.inquirer.net/1539249/in-the-know-the-2016-comeleak.

[49] Janvic Mateo, “Year of hackers: Bangladesh bank heist, Comeleak,” *The Philippine Star,* January 6, 2017, https://www.philstar.com/headlines/2017/01/06/1659976/year-hackers-bangladesh-bank-heist-comeleak.

[50] Disini & Disini Law Office, “A Win for ICT: Towards a Department of Information and Communications Technology.”

[51] Macasaet, “DICT: Is it really necessary for PH transformation?”

[52] Cisco, “Cisco 2018 Asia Pacific Security Capabilities Benchmark Study,” 32, https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf.

[53] Newsbytes.PH, “Study: 35% of cybersecurity solutions used by PH firms outdated,” December 11, 2021, https://newsbytes.ph/2021/12/11/study-35-of-cybersecurity-solutions-used-by-ph-firms-outdated/ https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-study-vol-2-report.pdf?ccid=cc000160&oid=rptsc027923&dtid=odicdc001478.

[54] First, Cisco reported that Philippine companies are shifting to modern technology. https://www.bworldonline.com/corporate/2021/12/13/416986/cisco-says-phl-companies-shifting-to-modern-cybersecurity-technologies/. Second, Surf Shark reported that the Digital Quality of Life in the country has developed to become 48th in the world in 2021, which is 18 places higher than that in 2020. https://surfshark.com/dql2021?country=PH.

[55] Arjay L Balinbin, “Cyberattacks pose clear and present danger to PHL,” *Business World,* March 22, 2022, https://www.bworldonline.com/top-stories/2022/03/22/437360/cyberattacks-pose-clear-and-present-danger-to-phl/.

[56] Sophos, *The Future of Cybersecurity in Asia Pacific and Japan - Culture, Efficiency, Awareness,* August 2019.

[57] Business Mirror, “‘IT security budget stagnant despite rise in cyber attacks,’” April 1, 2021, https://businessmirror.com.ph/2021/04/01/it-security-budget-stagnant-despite-rise-in-cyber-attacks/.

[58] Secure Connections and The Asia Foundation, *Cybersecurity in the Philippines: Global Context and Local Challenges,* March 2022, 15.

[59] Secure Connections and The Asia Foundation, *Cybersecurity in the Philippines: Global Context and Local Challenges,* 22.

[60] Secure Connections and The Asia Foundation, *Cybersecurity in the Philippines: Global Context and Local Challenges,* Foreword.

[61] Simon Kemp, “Digital 2022: Global Overview Report, *Data Reportal,* January 26, 2022, https://datareportal.com/reports/digital-2022-global-overview-report.

[62] Statista, “Number of social media users in the Philippines from 2017 to 2020, with forecasts until 2026,” https://www.statista.com/statistics/489180/number-of-social-network-users-in-philippines/.

[63] Kyle Chua, “PH remains top in social media, internet usage worldwide - report,” *Rappler,* January 28, 2021, https://www.rappler.com/technology/internet-culture/hootsuite-we-are-social-2021-philippines-top-social-media-internet-usage/.

[64] Speedtest, “Philippines’ Mobile and Fixed Broadband Internet Speeds,” https://www.speedtest.net/global-index/philippines#fixed.

[65] Raymond Carl Dela Cruz, “Giant leap in ICT infra makes people more connected in 2021,” *Philippine News Agency,* December 31, 2021, https://www.pna.gov.ph/articles/1164219.

[66] Richmond Mercurio, “DICT’s free WiFi rollout continues,” *The Philippine Star,* October 10, 2021, https://www.philstar.com/business/2021/10/10/2132980/dicts-free-wifi-rollout-continues.

[67] Dela Cruz, “Giant leap in ICT infra makes people more connected in 2021.”

[68] National Cybersecurity Plan 2022, 24.

[69] PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014) 154.

[70] Singer and Friedman, *Cybersecurity and Cyberwar,* 154-155.

[71] Priam Nepomuceno, “AFP starts week-long cyber defense exercise,” *Philippine News Agency,* November 8, 2021, https://www.pna.gov.ph/articles/1159105.

[72] National Cybersecurity Plan 2022, 46.

[73] 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-revealschinese-apt-groups-may-have-been-entrenched-in-some-servers-fornearly-a-decade-using-little-known-linux-exploits/.

[74] ABS-CBN News, “PH target of 10-year Chinese cyber espionage: group,” *ABS-CBN News*, May 20, 2015, https://news.abscbn.com/nation/05/20/15/ph-target-10-year-chinese-cyber-espionagegroup.

[75] Singer and Friedman, *Cybersecurity and Cyberwar,* 92-94.

[76] Singer and Friedman, *Cybersecurity and Cyberwar,* 99-101.

[77] Francis C Domingo, “Strategic Considerations for Philippine Cyber Security,” *Stratbase’s Albert Del Rosario Institute Occasional Paper* 9.1, NA (2016): 8.

[78] Marvin Waschke, *Personal Cybersecurity: How to Avoid and Recover from Cybercrime* (New York, Apress, 2017) 193-219.