SEPTEMBER 2023

SPARK®

the key link between IDEAS and ACTION

QUARTERLY
PUBLICATION
OF THE
ADRInstitute

CYBER DEFENSE POSTURE AND ITS COLLECTIVE SECURITY IMPLICATIONS FOR THE PHILIPPINES

adrinstitute.org

CYBER DEFENSE POSTURE AND ITS COLLECTIVE SECURITY IMPLICATIONS FOR THE PHILIPPINES

The Philippines has faced numerous challenges in implementing a national cybersecurity strategy. Since 2016, the country has experienced several setbacks due to varying organizational mandates, limited resources, and allegations of irregularities. Because of these reasons, the previous National Cyber Security Plan (2017-2022) was barely adopted.

At present, the Marcos administration has finalized its national security policy and looks forward to completing the national security strategy by 2024. This will define the administration's philosophy and view on cybersecurity. Meanwhile, the Department of Information and Communications Technology (DICT) is developing its own national cybersecurity agenda. A review of these plans shows the differences in philosophies and approaches and the lack of a consolidated roadmap and metrics on how to determine its milestones. Moreover, various public agencies and the private sector are developing their own cybersecurity plans, thus showing a siloed and uncoordinated approach.

This paper intends to address the cycle of policy fragmentation in this domain by proposing the adoption of a cyber defense posture (CDP) for the Philippines. This requires the government to adopt a collective defense paradigm by encouraging critical sectors to be part of the national digital strategy. Examples from countries like Canada, the United Kingdom and the United States can provide valuable insights on how to pursue a CDP. For instance, through public sector leadership and incentives, the private sector can be part of this initiative of forging common sectoral standards, sharing of information, and sandboxing agreements. Another highlight of a CDP is to encourage policy makers and security planners to go beyond the usual legal-criminal domain. This new paradigm underscores the importance of resilience, thus encouraging governments to invest in preparation, innovation, continuity, and deterrence. Overall, these views on the CDP provide stakeholders with insights on how to operationalize the "whole-of-society concept" of cyber security. In particular, the study intends to answer the question: "*How can the Philippine government adopt a collective defense paradigm? What are the requirements to pursue a CDP?*"

To do this, the paper will highlight the opportunities for the country, especially now that the current administration has articulated its desire to pursue a digital transformation strategy. To further argue for the need to adopt a CDP, the paper will also discuss the weaponization of cyberspace as shown in the experiences of Taiwan and Ukraine. At the end of the discussion, the paper will put forward recommendations for the country's policymakers and planners on how to adopt a CDP.

The Philippines: Addressing Challenges and Creating Opportunities

The Philippines' foray into digital transformation (Dx) is inevitable. No less than President Ferdinand Marcos, Jr. articulated this vision in his first State of the Nation Address (SONA) in July of 2022. Prior to this, the country witnessed an upsurge in digital payments, the use of social media, and increasing competition within the Asia Pacific region. There have been previous initiatives to jumpstart the country's Dx journey. However, the COVID-19 pandemic and changing political priorities have hampered its realization. For these reasons, the Philippine Congress has articulated its desire to enact laws on e-government and freedom of information to underscore the state's commitment. Nevertheless, this optimism will be for naught if we miss out on the traditional metrics and experiences in this domain. At this point, the discussion will focus on the United Nations' E-Government Development Index (EGDI) and the Global Cybersecurity Index (GCI). These indices are useful guides to determine the starting point of the country's digital transformation initiative and ensure a secure digital ecosystem.

E-Government Development Index (EGDI)

The E-Government Development Index presents the state of e-government of UN member states. The EGDI assesses the capacities of countries to deliver essential online public services. Moreover, the EGDI is a weighted average of the three most significant dimensions of e-government namely: (1) scope and quality of online services (Online Service Index-OSI), (2) development status of telecommunications infrastructure (Telecommunications Infrastructure Index-TII), and (3) inherent human capital (Human Capital Index-HCI).

Drawing from the EGDI 2022, the Philippines ranked 89 out of 193 countries with a weighted average score of 0.65230 (Table 1). While the score is above the EGDI world average of 0.6102, the regional average of 0.6493, and t he sub-region average of 0.6405, the country's current position still lags behind its ASEAN peers.

E-Government Index Score : **Philippines**

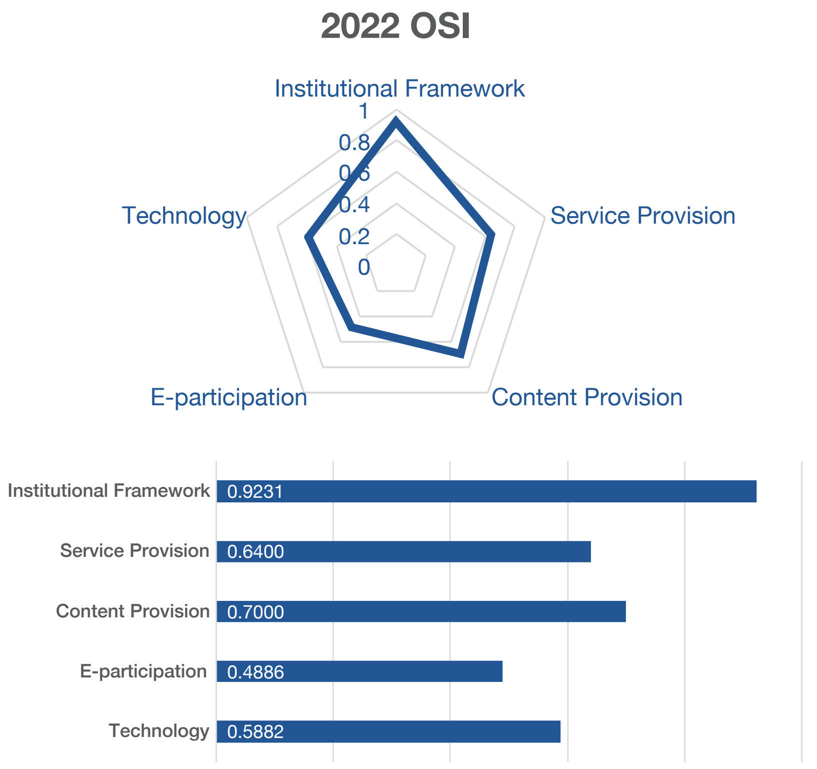
Table 1

E-Government Development Index	2022	2020	2018	2016	2014	2012
Philippines (Rank)	89	77	75	71	95	88
Philippines (Value)	0.65230	0.68920	0.65120	0.57655	0.47681	0.51303
E-Government Development Index	**2010**	**2008**	**2005**	**2004**	**2003**	
Philippines (Rank)	78	66	41	47	33	
Philippines (Value)	0.46373	0.50010	0.57211	0.52595	0.57364	

Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

Online Service Index 2022 : **Philippines**

Figure 1



Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

SEPTEMBER 2023 | VOLUME 16 ISSUE 3

FEATURES

ON THE COVER

Cover, title page, contents page and page 19: forbes.com/sites/forbestechcouncil/2022/02/08/cyber-defense-in-2022-business-as-usual/?sh=4c122fdb767e; afr.com/technology/cyber-security-is-a-fact-of-modern-life-and-it-needs-to-be-treated-that-way-20230605-p5ddyj; kaspersky.com/about/policy-blog/from-cybersecurity-to-cyber-defense; and simplilearn.com/top-cyber-security-projects-article

ABOUT THE AUTHOR

Sherwin E. Ona, Ph.D.

is a non-resident fellow of Stratbase ADRi and a senior academic fellow of the Philippine Public Safety College. In addition, Dr. Ona is a module director and lecturer on cyber defense policies at the National Defense College of the Philippines and serves as a consultant for the National Security Council. Finally, he is an associate professor of political science and development studies at De La Salle University

CONTENTS

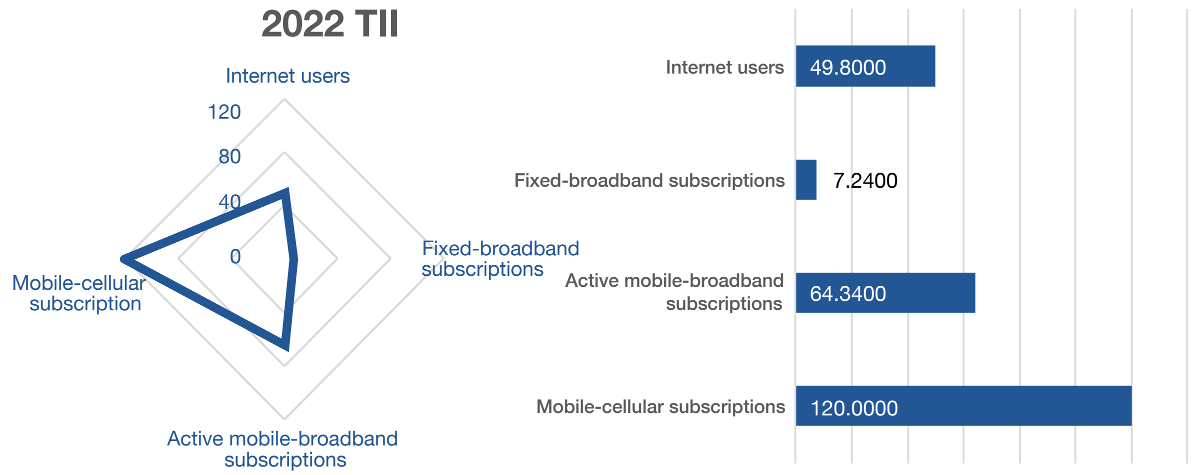
cyber security

Breaking it down to the three dimensions of the EGDI, the Philippines scored a value of 0.63030 for the OSI in Figure 1. The OSI used metrics such as institutional framework, service provision, content provision, e-participation, and technology. Moreover, the Philippines scored above the world, region, and sub-region averages for 2022, which were 0.5554, 0.6137, and 0.5955, respectively.

For the TII (Figure 2), the Philippines scored a value of 0.5638 by using the metrics of internet users, fixed-broadband subscriptions, active mobile-broadband subscriptions, and mobile-cellular subscriptions. In contrast to OSI, the Philippines scored below the world, region, and sub-region averages for TII, which were 0.5751, 0.6166, and 0.6324, respectively.

Telecommunication Infrastructure Index 2022 : **Philippines**

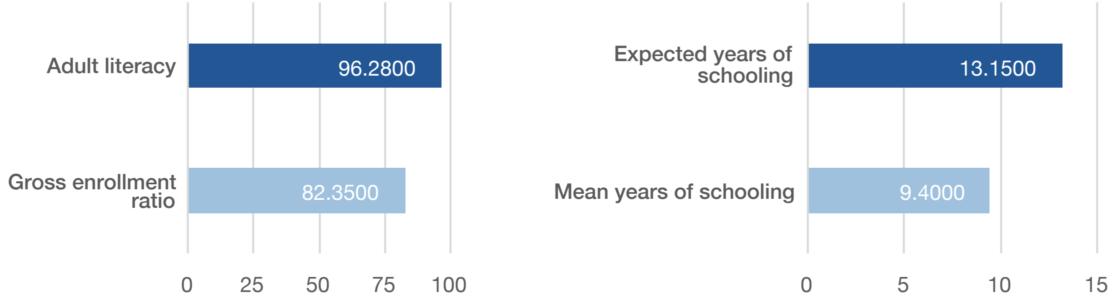
Figure 2



Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

Human Capital Index 2022 : **Philippines**

Figure 3

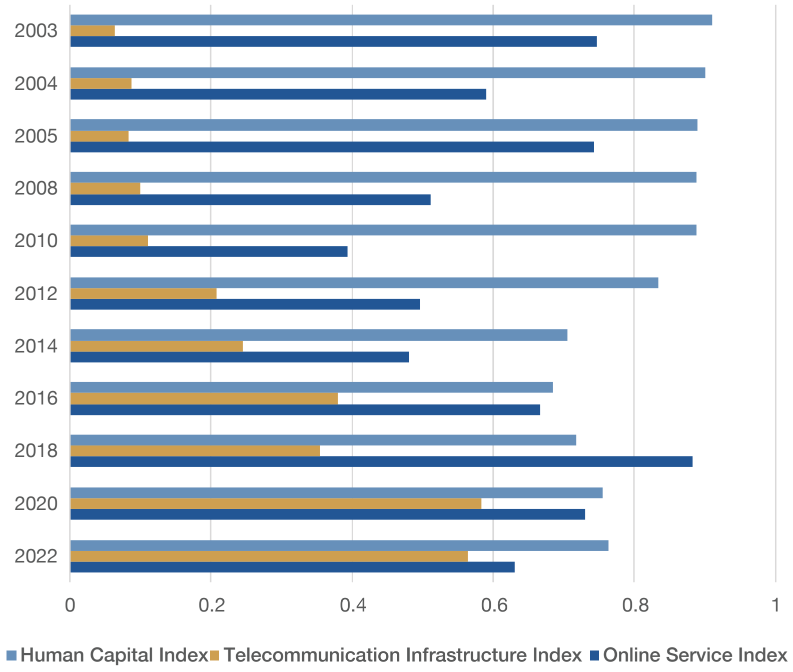


Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

Lastly, for the HCI (Figure 3), the Philippines scored 0.76290 which considered variables such as adult literacy, gross enrollment ratio, expected years of schooling, and years of schooling mean. In this Index, the Philippines scored above world, region, and sub-region averages, which were 0.7001, 0.7175, and 0.6937, respectively. Figure 4 provides a comparison of the three dimensions of e-government from the period between 2003 and 2022.

EGDI Dimensions Score 2003-2022 : **Philippines**

Figure 4



Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) published by the International Telecommunications Union (ITU) measures the commitment of 193 ITU member states (and the State of Palestine) to cybersecurity. This commitment is assessed through each country's level of development using five pillars namely: (1) Legal Measures; (2) Technical Measures; (3) Organizational Measures; (4) Capacity Development, and (5) Cooperation – which are all aggregated into an overall score. The Index aims to help countries identify gaps and encourage the inclusion of good practices that will ultimately provide useful insights to develop a strong national cybersecurity posture.

Global Cybersecurity Index Score : **Philippines**

Table 2

Global Cybersecurity Index	2020	2018	2017	2014
Philippines (Rank)	61	58	37	17
Philippines (Score)	77*	0.643	0.594	0.353

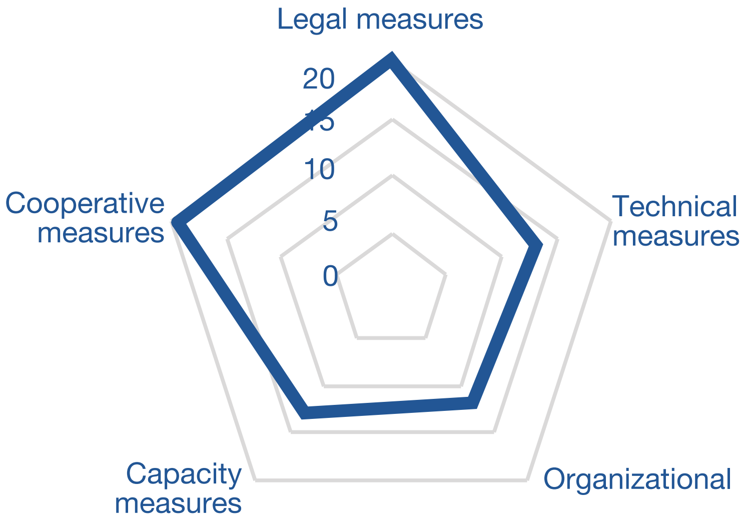
Note. Weightages differ from the previous iterations and were based on expert recommendations

Source: The International Telecommunications Union (2020)

Based on the GCI 2022, the Philippines ranked 61 out of 194 countries assessed with an overall score of 77. As seen in Figure 5, it was relatively strong in the pillars of legal and cooperative measures, scoring a perfect 20 on the former. It comes as no surprise since the Philippines has already passed laws and other regulatory frameworks that promote a safe and secure cyberspace. Laws like the Cybercrime Prevention Act, E-Commerce Act, Anti-Child Pornography Act, Data Privacy Act, the National ID law, and the recently passed SIM Card Registration Act are some of these legal and regulatory instruments. Furthermore, the Philippines scored 19.41 in cooperative measures. As cybersecurity is often seen as a transnational issue, it requires cross-border cooperation. In this case, the Philippines has already signed multilateral and bilateral agreements like the Budapest Convention

Global Cybersecurity Index 2022 Scores, Based on the Five Pillars : **Philippines**

Figure 5



Development Level:
Developing Country

Area(s) of Relative Strength:
Legal, Cooperative Measures

Area(s) of Potential Growth:
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Measures	Cooperative Measures
77.00	20.00	13.00	11.85	12.74	19.41

Source: United Nations Department of Economic and Social Affairs (UNDESA), 2022

on Cybercrime. The country also joined the ASEAN ministerial meetings on developing an ASEAN-wide CERT cooperation framework. Furthermore, the US-Philippines Mutual Defense Treaty's new Bilateral Defense Guidelines include cyber defense and cybersecurity cooperation.

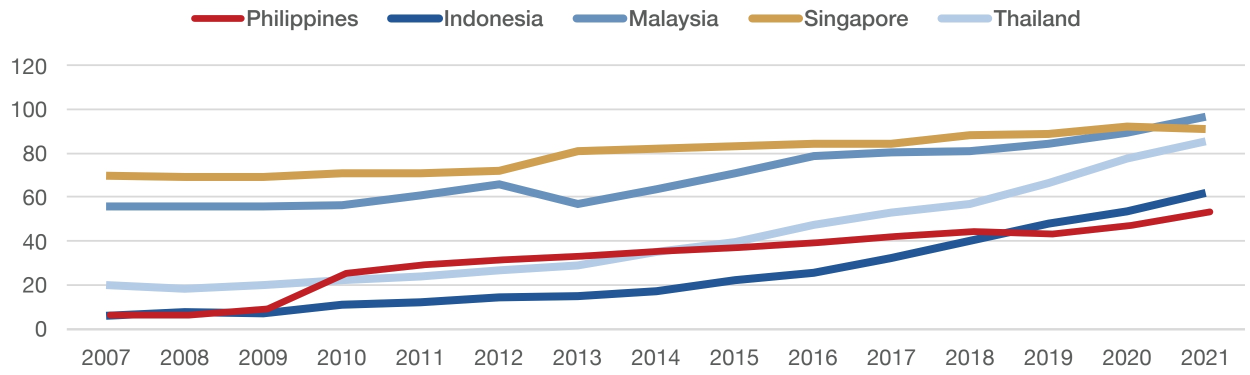
Based on the EGDI, the Philippines ranked above the global average for telecommunications and online services. However, there is a noticeable fluctuation in the country's ranking from 2016 to 2022. This is probably due to the changing nature of e-government initiatives since countries are moving away from stand-alone/organization-centric practices towards more integration and interoperability of services. This is consistent with the concept of Dx. Meanwhile, the country's GCI ranking fared well in the legal-regulatory and cooperative aspects of the index. However, it lags in the technical, organizational, and capacity aspects. These figures show that the country's Dx aspirations should focus more on developing integrated services and prioritize the development of its technical and organizational capacities.

a. Opportunities for the Philippines: Connectivity, Digital Payments, and Social Media usage

The country's digital transformation agenda depends on its ability to develop its digital infrastructure. Figure 6 shows the comparison of individual internet usage (% of the population) of 5 ASEAN countries namely Indonesia, Malaysia, Singapore, the Philippines, and Thailand. Interestingly, the Philippines showed the biggest increase in over a year in internet usage in 2010, faring better than the other two upper middle-income countries of Indonesia and Thailand, which had lower internet usage in 2010-2013 and 2009-2017, respectively. Although the expansion of internet usage in the Philippines has now fallen behind the other four countries, it was able to expand from just 6% in 2007 to 53% in 2021.

Individuals Using the Internet, Percent of Population : **ASEAN 5**

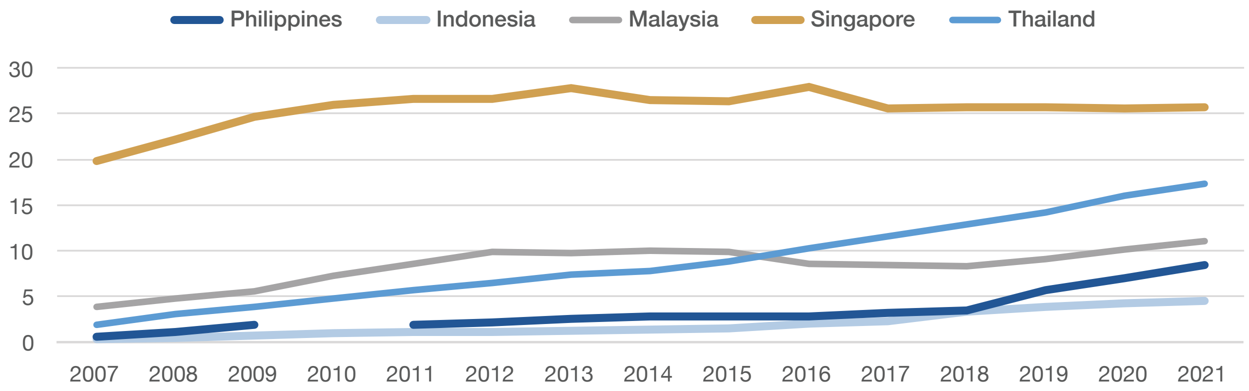
Figure 6



Source: International Telecommunications Union (2022)

Fixed Broadband Subscriptions, 2007-2021 per 100 People : **ASEAN 5**

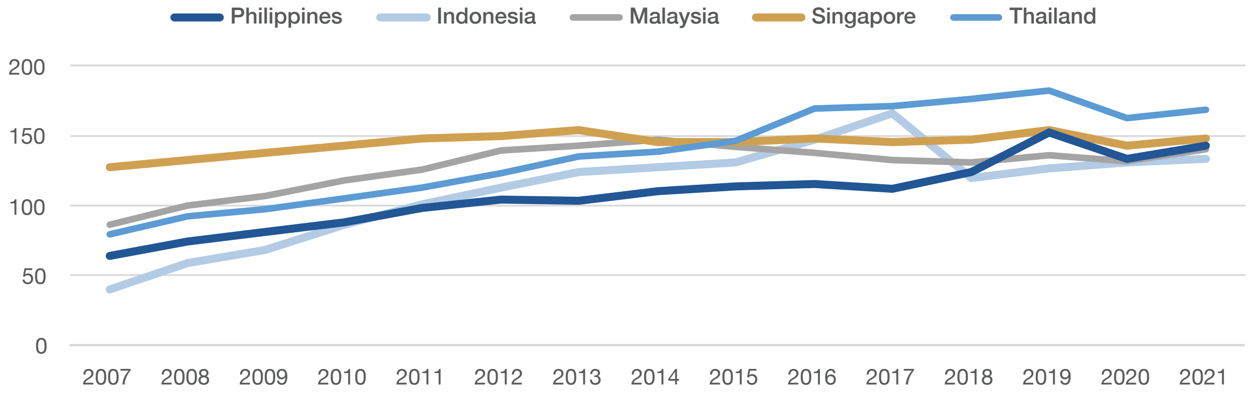
Figure 7



Source: International Telecommunications Union (2022)

Mobile Cellular Subscriptions , 2007-2021 per 100 People : **ASEAN 5**

Figure 8



Source: International Telecommunications Union (2022)

Figure 7 presents the fixed broadband subscriptions (per 100 people) of the ASEAN 5 countries from 2007 to 2021. Here, subscriptions have steadily increased from 2011-2018 for the Philippines and experienced a relatively sharp increase in 2019 with a value of 5.71.

Figure 8 provides the comparison of mobile cellular subscriptions (per 100 people) of the ASEAN 5 from the period between 2007 and 2021. Here, the Philippines had a steady increase from 2007 up to 2009. In 2020, it had a significant drop from a score value of 152 in the previous year to 133. Nonetheless, subscriptions did increase in the subsequent year.

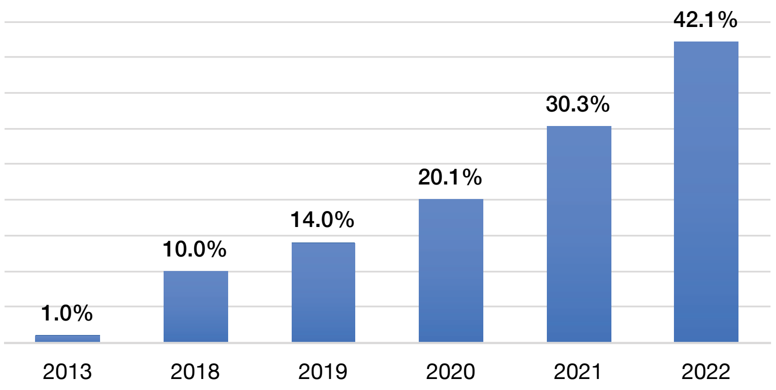
Digital Payments in the Philippines

Another exciting development is the growth of the country's financial technology (FinTech) industry. No less than the Bangko Sentral ng Pilipinas (BSP) recognized this opportunity and encouraged industry players to "strike while the iron is hot" and stressed the importance of tapping the "innovation DNA to create worthwhile solutions". The BSP also noted that the pandemic has opened new opportunities for the FinTech sector and that it is essential for Filipinos to seize the moment (Lucas, 2021).

Around the world, access to digital financial services is expected to increase. For Filipinos, this will result in new ways of paying, saving, and investing their money. The BSP's 2022 Status of Digital Payments shows that there was an accelerated growth in the use of digital payments from 2018 to 2022. As shown in Figure 9, the share -- in terms of volume -- of digital payments over retail payments has grown considerably to 42.1% in 2022, an 11.8% increase from 2021 and 22% from 2020 (BSP, 2023).

Share of Digital Payments by Volume

Figure 9



Source: Bangko Sentral ng Pilipinas (2023)

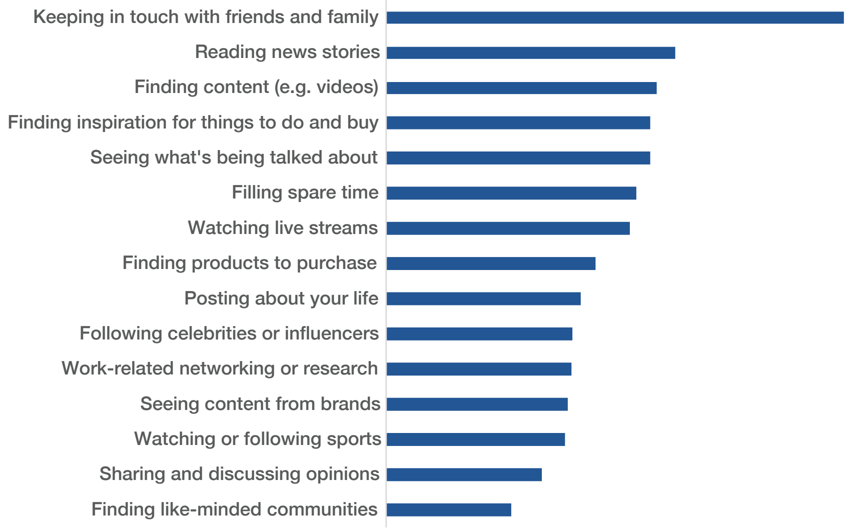
Social Media Usage in the Philippines

According to the report by US-based Meltwater and We Are Social, 72.5% of Filipinos (84.5 million) have a social media account. It was also reported that Filipinos spend an average of three hours and 43 minutes on social media per day.

Moreover, as seen in Figure 10, 69.2% of Filipino social media users' primary reasons for using social media platforms are mainly to keep in touch with family and friends. This is followed by reading news stories with 47.3%, and finding content with 44.9%, while online shopping and seeing what's being talked about or what's trending are both at 44.1%.

Main Reasons for Using Social Media for Filipinos

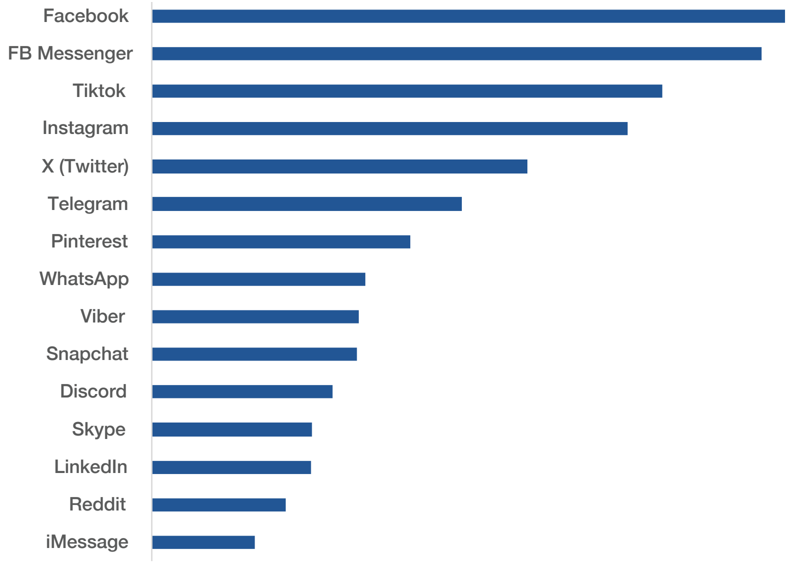
Figure 10



Source: Meltwater (2023)

Most Used Social Media Platforms for Filipinos

Figure 11



Source: Meltwater (2023)

Box 1 : The Country’s Strengths and New Opportunities

- **The digital native Filipino**: According to “We Are Social” and “Hootsuite,” Filipinos spent the most time on social media worldwide in 2020, with an average of 4 hours and 15 minutes a day. The country also logged the highest Internet usage with 11 hours a day. Specifically, “We are Social” pegged the country’s internet users at 73 million as of Jan. 2020.

- **The pervasiveness of social media dominance**: A 2019 SWS survey says that almost half of Filipino adults (45%) nationwide have access to and are using the Internet with 29.4 million having a Facebook account. 24% of this group also read the news daily through FB.

- **Rise of the millennial workers’ cohort**: A younger workforce would lead to a cohort of digitally savvy workers. It is expected that the millennial cohort will make up 75% of the global workforce by 2030 (SWS, 2020). This trend is expected to result in increased productivity and higher demand for flexible working arrangements.

- **The Philippines’ satisfactory rating in E-Government and Open Data:**The UN’s 2022 E-Government Development Index (EDGI), rated the country as 89th out of 193 countries. In addition, the Open Data Barometer continues to recognize the Philippines as one of the top performers for its openness and data transparency with its 22nd rank out of 115 middle-income Asia-Pacific countries (ODB, 2020).

- **Growth in digital payments**: In less than a decade, the volume of digital payments has increased significantly. The pandemic has also shown the potential of digital payments. Aside from its transactional side, digital wallets can also encourage savings and subscriptions to insurance services.

Figure 11 gives an overview of the top social media platforms in the country. Among the social media platforms most favored by Filipinos, Facebook remains on top with 95.7%, followed by Facebook Messenger with 92.1%, the rising popular platform of TikTok with 77.2%, Facebook’s sister app Instagram with 71.9%, and the microblogging site Twitter (now X) with 56.7%. As Facebook retains its popularity in the Philippines, it is not surprising that the country’s top cellular networks offer the social platform for free to their subscribers.

In summary, the Philippines’ ability to adopt Dx is underpinned by its pervasive use of social media and digital payments, its young workforce, and the potential of its telecommunications industry. Furthermore, the government’s emphasis on digitizing its services as well as its growing consciousness on cybersecurity and privacy are crucial factors that can drive Dx. Box 1 summarizes these points.

b. Challenges: Cybercrime and Disinformation

As more countries adopt Dx as a strategy, it should not be a surprise that an increase in digital crimes would occur. For instance, the Global Risks Report published by the World Economic Forum (2023) places cybersecurity in the top 10 global, current, and future risks. According to the online periodical Cybersecurity Ventures, it is estimated that the annual costs of cybercrime will hit $10.5 trillion by 2025. Consequently, around 45% of organizations worldwide will be impacted in some way by attacks on supply chains (Ene, 2023).

The Philippines is not exempt from this phenomenon. The country was ranked by Kaspersky Security Network as the second most digitally assaulted nation in 2022, with the Philippines receiving 46.8% of the recorded attacks. The report also mentioned that “drive-by” downloads and social engineering are the most favored methods used to spread malware (Ronda, 2023). In 2023, the PNP-Anti Cybercrime Group said that more than PHP155 million was lost to various online scams from January to August and that the agency received over 8,000 complaints in the same period (Argosino, 2023).

The Philippines – A Petri Dish for Disinformation

In an interview, Cambridge Analytica whistleblower Christopher Wylie said that they regard the Philippines as a “petri dish” for disinformation techniques. He further stated that the country was a good testing ground since it meets three underlying conditions, namely: (1) high social media usage, (2) questionable rule of law, and (3) corrupt politicians. The country’s weak regulatory infrastructure and high social media usage have made it possible for Cambridge Analytica to test out these strategies before deploying them in Western economies (Occeñola, 2019). Wylie also revealed that around 87 million Facebook users’ data was harvested and targeted for political campaigns. Of these numbers, 1.2 million users came from the Philippines, the second highest after the United States (Occeñola, 2019).

Learning from Prevailing Work and Experiences

After examining the challenges and opportunities for the Philippines, this section is concerned with how cyberspace is being weaponized in the name of the national interest. This will be followed by a discussion on how a CDP framework can be developed using passive and active cyber defense concepts and the practices of three selected countries. Finally, the paper will put forward recommendations on how the Philippines can adopt a CDP.

Weaponization of Cyberspace: Lessons from Ukraine and Taiwan

The weaponization of cyberspace is evident in today’s geopolitical competition. The internet has become a vehicle for launching cyberattacks and disinformation campaigns aimed at weakening an adversary’s resolve during wartime. The Russian aggression against Ukraine showed cyber and information operations are combined with physical attacks to disable critical targets. For instance, the 2022 invasion resulted in tens of thousands of satellite modems in Ukraine and Europe being disabled by attacks. In addition, Ukrainian websites were subjected to DDOS attacks, and their internet services were temporarily disrupted in an attack against Ukraine’s telecommunications providers. This coincided with the release of Russian wiper malware against Ukrainian systems. There were also reports that Russia launched a cyber-attack against Starlink terminals. However, this was quickly addressed by SpaceX through a system update (Duffy, 2022).

Another ominous example is the rising tensions in the South China Sea and the Taiwan Strait. This has resulted in an astounding display of gray and hybrid warfare in the region. Sophisticated cyberattacks combined with elaborate disinformation campaigns have sought to deny access to services and information as well as undermine democratic institutions. Taiwan is no stranger to this phenomenon and has witnessed firsthand the ferocity of these attacks. For instance, during the 2020 presidential elections, it has been reported that Taiwan experienced 20-40 million attacks per month (Hsini & Tien-Shen, 2018). Similarly, during the visit of high-profile US officials in 2022, its government reported an astonishing 50 million attacks per day (60 Minutes, 2022).

These ominous events clearly show that Taiwan is a target of cyber coercion intended to spread fear, panic, and confusion to intimidate its people (Manantan, 2020). Allegedly perpetrated by the People’s Republic of China (PRC), the weaponization of cyberspace has become a hallmark of asymmetric and gray zone warfare not only in Taiwan but in Hong Kong and Southeast Asia as a whole (Curtis, 2021). These insidious acts are intended to undermine Taiwan’s democratic institutions, leading to a possible invasion, which the PRC has never denied.

Despite being one of the most attacked in cyberspace, Taiwanese institutions are considered among the best in the world in terms of cyber defense. Since the late 1990s, Taiwan has been quick to recognize that new cyber threats would require a consolidated government response. It also underscored the need to better prepare its society by labeling cybersecurity as a national security concern. Lately, it has developed a unified defense paradigm that involves the government, the private sector, and its citizens (NCSP, 2021-2024).

Examining the CDP Concept

The continuous weaponization of cyberspace shows that its impact is becoming societal rather than organizational. Malicious actors, whether state or non-state, are continuously innovating and exploiting system vulnerabilities. Sophisticated attacks are aimed at disrupting services and infrastructure, and undermining institutions. Moreover, the use of artificial intelligence and social engineering is now allowing for the "hacking the human to hack the network" and the rapid spread of disinformation. Unfortunately, many policymakers and defense planners treat cyber as a technical domain, where the expertise needed is specialized and highly technical. This view also dismisses the socio-technical aspect of cyber defense.

Therefore, it is crucial to treat cyberspace as both a contested domain and a venue where freedoms and development can be advanced. A CDP must adopt a national security-oriented view that goes beyond the usual organization-based management of information systems (MIS) techniques like cyber hygiene and firewalls, among others. A CDP should complement this "castle principle"- the act of strengthening the technical-organizational aspect of cyber security through the development of doctrines and plans. These actions and outputs underscore the importance of defending a nation's citizens by protecting its critical infrastructure and embracing the concept of resilience. Moreover, this approach requires a whole-of-society strategy that can address emerging threats and mitigate the adverse impact of disruption and disinformation.

Box 2 : Passive Cyber Defense: A Snapshot

PCD is focused on strengthening the security of systems and data. Below are several practices attributed to PCD:

- **Early Warning and incident notification** - Cyber agencies are tasked with providing warnings about impending cyber-attacks, the spread of malware, and misinformation through advisories and coordination.

- **Provide services to government and the private sector** - Cyber agencies offer a range of digital/cyber services like the protection of its domain name server (DNS), quick reaction services to contain an attack, as well as the conduct of cyber training exercises among others.

- **Emergency Response and law enforcement** - Create or strengthen the capabilities of national and sectoral computer emergency response teams (CERTs) and law enforcement agencies.

- **Provide a venue for sharing** - governments and its partners provide information and advisories to various sectors regarding threats and attack morphologies.

- **Policy Advocacy and Development** - Develop digital policies that will foster the adoption of cyber security practices at all levels of society (i.e., Whole of nation, organizations, groups, households, and individuals).

Box 3 : Active Cyber Defense: A Snapshot

Active Cyber Defense (ACD) concept allows governments to offensive cyber capabilities for deterrence and retaliation. Examples of these capabilities are as follows:

- Develop capabilities that will allow defenders to hack back at an adversary. This calls for creating the same capabilities that adversaries have.

- Having the ability to mount active surveillance operations of adversaries and their cohorts.

- Open the option of combining cyber with kinetic attacks. This is usually seen in wartime.

- Forging alliances for joint cyber operations against an adversary.

Passive Cyber Defense (PCD)

This approach to cybersecurity is often viewed as an organizational-centric, MIS-oriented strategy that aims to protect customers, ensure access to an organization's products and services, as well as protect its intellectual property. Its main goal is to minimize the effectiveness of cyber threats through security engineering, configuration management, vulnerability, and risk assessment. Furthermore, passive techniques include disaster recovery and training of users (Denning, 2013). Box 2 provides an overview of PCD.

At the organizational level, PCD's concerns are the following (Addington & Manrod, 2019):

a. *Confidentiality of Information* - Organizations are tasked to prevent theft of personal information and intellectual property.

b. *Integrity of Data* - Organizations must prevent unwarranted manipulation of data.

c. *Availability of Information* - An organization's services and information must be accessible on demand.

In addition, traditional cybersecurity requires a security governance framework that includes risk management and compliance with mandated standards such as COBIT, ISO 2007, and the NIST 800x. It also ensures the authenticity of information and its non-repudiation quality (Whyte and Mazanec, 2019) (Addington & Manrod, 2019). Several advocates of PCD propose that its practice go beyond organizational boundaries and adopt information sharing with partners. This can be seen in the creation of industry/sectoral practices and standards (i.e., banking, telecoms, health, etc.) as well as the integration of its value chains. Known as collective cyber defense (CCD), this approach underscores the value of collaboration based on threat assessment and information sharing especially on cybercrimes, hacktivism, and terrorism (Skopik et al., 2016). Another important aspect of CCD is the ability to establish the attack morphology. This technique requires the defender to establish the context and nature (quantity and quality) of the attack as well as the intent of the attacker. The results of this are expected to be addressed through regulation and governance (Addington and Manrod, 2019) (Skopik et al., 2016). Overall, these strategies are aimed at fostering resilience through information exchange, joint threat assessment, and resource sharing. It also requires a strong cyber forensic capability.

For its part, the private sector plays a crucial role in this passive/collective defense stance. Note that significant investments have been made in cybersecurity. However, most of these investments are focused on protecting data, systems, and intellectual property. A collective defense paradigm will entail the identification of critical sectors (i.e., banking, telecoms, health, etc.) and create a common space for sharing information and best practices as well as developing threat assessments, among others.

Active Cyber Defense

It can be argued that active cyber defense (ACD) is an important component of a collective defense paradigm. Proponents of ACD recognize the importance of securing networks and protecting critical infrastructure. However, it takes off from its passive counterpart by adopting a more proactive approach. A prominent quality of ACD is the identification and neutralization of threats while infrastructure targets are strengthened (Denning, 2014). Proponents of ACD characterize threats as campaigns that can be instigated by nation-states and their allies. This in turn shifts away from a purely law enforcement viewpoint and adopts the national security paradigm. Furthermore, ACD adopts a "hack-back" mentality that includes the development and use of offensive cyber capabilities. Examples of these offensive capabilities are as follows (Fanelli, 2016) (Whyte & Manzanec, 2019):

a. *Ability to exploit the vulnerabilities of an adversary's information systems and resources* - This capability pertains to the ability of a defender to know an attacker's intent, techniques, and vulnerabilities. This technique intends to hack-back against an attacker.

b. *Having the ability to alter access controls and deploy decoys that can mislead an attacker* - This is usually referred to as the honey pot technique which intends to lure an attacker to a controlled environment to know more about its capabilities.

c. *Increasing the cost of an attack to the attacker through political, economic, and legal means* - This is part of the concept of deterrence which believes that attackers can be deterred through economic sanctions, political consequences, and legal actions.

Overall, ACD adopts the idea of passive defense but tends to be more proactive in addressing the sources of the cyber threats. It generally espouses the idea of deterrence and proposes that offensive capabilities be developed and used persistently to degrade an adversary's malicious cyber abilities. The idea of proactive defense also gives the government the responsibility of coordinating national cyber defense efforts with its partners and defense allies.

Country Examples

Canada

In 2016, the Canadian government sought to understand the changing cyber environment by engaging its major stakeholders. Input from its federal agencies, the private sector, academics, as well as security experts, revealed the key issues of cyber security, namely: (a) Cybersecurity should protect the personal data of citizens, thus emphasizing the importance of privacy; (b) Acknowledge the challenges of its law enforcement agencies in addressing cybercrimes; (3) Recognize the need for strong leadership from the federal government and (4) Address the skills and knowledge gaps and (5) There is a need to develop standards and legislation. Given these, the National Cybersecurity Strategy (NCSS) was launched in 2018. The strategy emphasized that a secure digital ecosystem is a prerequisite for ensuring economic growth and prosperity. As such, the NCSS is anchored on three themes namely (Government of Canada, 2018):

a, *Security and Resilience* - This theme emphasizes the importance of collaborative action with partners and the improvement of the country's security capabilities. It also underscores the need to defend critical infrastructure as well as the private sector.

b. *Innovative and Adaptive Cyber Ecosystem* - Developing skills and advancing knowledge are the key concerns of this theme. It envisions Canada as a global leader in cybersecurity.

c. *Effective Leadership, Governance, and Collaboration* - This theme also recognizes the importance of domestic leadership in Canada and collaboration with the private sector and local governments, aside from its being a global innovator,

In addition, the NCSS highlighted the government's commitment to protecting the country's critical infrastructure, rights, and freedoms online. It also underscored the public safety and national security implications of a vulnerable cyberspace. Thus, the government's National Cybersecurity Action Plan (2019-2024) provides detailed roles and responsibilities for various stakeholders. For instance, the plan highlights the lead role of the Department of Public Safety and Emergency Preparedness in conducting regular risk and vulnerability assessments for organizations, and in ensuring the resilience of industrial control systems (ICS). It also tasked the Canadian Center for Cyber Security to provide threat assessments to guide the government and the public. The center is also responsible for assisting Canada's finance and energy sectors in protecting their critical systems. Furthermore, the plan underscored the need to defend the country's digital ecosystem against espionage, sabotage, and foreign interference. For this, the Canadian Security and Intelligence Services is tasked to address its vulnerabilities and improve the country's overall situational awareness. The plan also entails the creation of a National Cybercrime Coordination Unit under the Royal Canadian Mounted Police. The unit is envisioned to coordinate police operations in the cyber domain and establish mechanisms for citizens and businesses to report cybercrimes.

On the aspect of innovation, the plan envisions the Government's key role in supporting research and helping local companies to develop cybersecurity products and services. It also recognizes the vulnerabilities of small and medium-scale enterprises. For this reason, the Innovation, Science, and Economic Development Canada (ISED), in cooperation with other public agencies, created the Cyber Security Innovation Network. The CSIN aims to serve as a collaboration hub for the government, private sector, and academic institutions that aims to increase commercialization and develop cyber skills nationwide.

United Kingdom

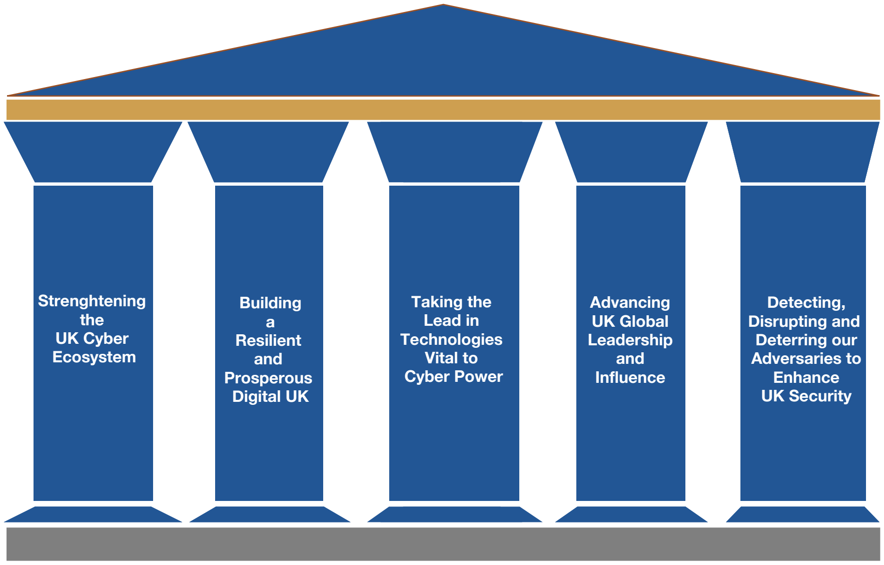
The key idea of the United Kingdom's national cyber strategy is the importance of cyber power as a component of national power and a source of strategic advantage. This entails the ability of the UK to promote its national interest while protecting its cyber environment. Furthermore, the UK understands that countries that can efficiently navigate the complexities of cyberspace will have to be more secure and resilient. These factors are vital in ensuring future prosperity of nations. This also means that the nation needs to be better prepared against cybercrimes and state-sponsored disruptions. The strategy also cites the transnational nature of cyberspace. It also acknowledges challenges posed by state and non-state actors such as criminals, hacktivists, terrorists, and other malicious actors. This further underscores the importance of international cooperation and need to develop active cyber capabilities through a national offensive cyber program as well as the establishment of a national cyber force.

Overall, the UK's strategy can be summarized through its 5 pillars (Figure 12), namely (HM Government, 2022):

a. *Pillar 1:* Strengthening the UK cyber ecosystem. This pillar calls for the continuous investment in its human resources and foster deeper

United Kingdom's National Cyber Strategy

Figure 12


Strenghtening the UK Cyber Ecosystem
Building a Resilient and Prosperous Digital UK
Taking the Lead in Technologies Vital to Cyber Power
Advancing UK Global Leadership and Influence
Detecting, Disrupting and Deterring our Adversaries to Enhance UK Security

Source: HM Government, 2022

partnerships with various societal sectors.

b. *Pillar 2:* Building a resilient and prosperous digital UK. The second pillar underscores the importance of preventing attacks by managing risks. It also highlights the concept of resilience and the need to recover from attacks.

c. *Pillar 3:* Taking the lead in the technologies vital to cyber power. The need to sustain the country's competitive advantage is the key idea in this pillar. For instance, its aspirations to develop next generation networks and security standards are prominently mentioned.

d. *Pillar 4:* Advancing UK global leadership and influence for a more secure, prosperous, and open international order. For this pillar, the strategy emphasizes the UK's role in promoting an open and free cyberspace. It also stresses the importance of sharing and collaborating with its allies on standards and risk mitigation, among others.

e. *Pillar 5:* Detecting, disrupting, and deterring adversaries to enhance UK security. The last pillar shows the country's commitment to protect and defend its infrastructure against malicious actors. This pillar also recognizes the importance of cyber in national security and law enforcement.

In addition, the UK government published its cyber security strategy (2022-2030). Meant to cover the public sector, it emphasizes the need to strengthen its infrastructure and build a strong foundation for cyber resilience. The strategy also calls for the creation of the Government Cyber Coordination Center (GCCC) that aims to harmonize cyber initiatives within the public sector, thus adopting a "defend as one" stance. This approach will be underpinned by the adoption of a cyber assessment framework which will act as a standard across departments and offices (HM Government, n.d.).

United States

In 2018, U.S. Department of Defense cyber posture adopted a defend-forward strategy which can be described as proactive cyber posture. Primarily designed to disrupt or halt malicious activities at their source (Goldman and Warner, 2021), this concept shifts the initiative to the side of the defender. In addition, this technique also emphasizes the importance of deterrence that can influence an adversary's cost-benefit calculus, thus affecting its decision process. Defend-forward also calls for the defender to gain the initiative by structuring the playing field to the disadvantage of the opponent (Goldman, 2022)
(White House, 2018).

To further elaborate the country's cyber posture, the White House released the National Cybersecurity Strategy in March 2023. It aims to redefine the government's vision for cyberspace and renew its commitment to ensure its security. Anchored on previous plans, the NCS emphasized the importance of the digital ecosystem as a venue to advance democratic values, and freedoms, as well as innovation and growth. It also laments the use of the Internet by authoritarian regimes as a tool for repression and surveillance, while stressing the current digital threats perpetrated by its adversaries. In addition, the NCS underscored two fundamental shifts in US cyber policy, namely: (a) Rebalance the Responsibility to Defend Cyberspace: This view highlights the role of small businesses, citizens, states, and local governments in securing cyberspace. (b) Realigning Incentives to favor Long-term Investments: This points to the role of the federal government to create incentives aimed at developing a secure and resilient cyberspace. These investments are also designed to promote collaborative stewardship, develop a diverse cyber workforce, and adopt standards. Overall, the NCS encapsulates its approach through the five pillars framework (Figure 13). These are the following (White House, 2023):

a. *Pillar One:* Defend Critical Infrastructure. This pillar underscores the importance of improving the cyber defense of critical infrastructure and the systems of the Federal government. It also promotes the concept of collective defense in partnership with the private sector as well as underscores the need to modernize its IT and Operational Technology systems.

b. *Pillar Two:* Disrupt and Dismantle Threat Actors. Consistent with the defend-forward strategy, the second pillar underscores the US desire to mitigate adverse cyber campaigns and dismantle entities that support them. Furthermore, the NCS states that the US can pursue diplomatic, criminal, informational, financial, and military actions against the perpetrators of these malicious activities. It also highlights the importance of sharing intelligence, improving its ability to mount disruptive campaigns against its adversaries, and denying access to its infrastructure.

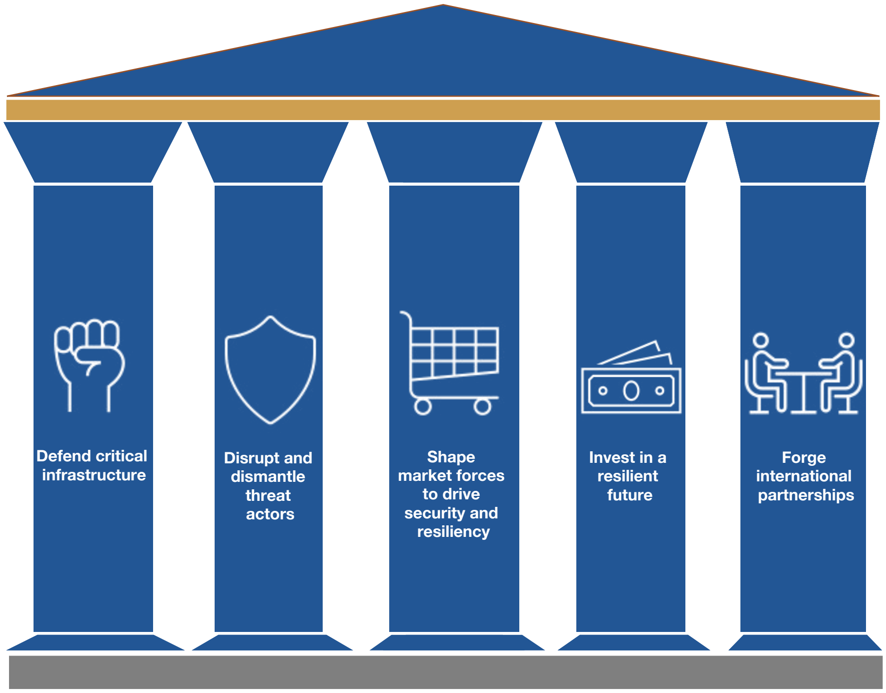
c. *Pillar Three*: Shape Market Forces to Drive Security and Resilience. This pillar recognizes the role of the market to drive the country's cyber resilience. It also points to the vulnerabilities of small businesses and organizations, as well as the need to streamline laws and regulations to enable resilience. Furthermore, this pillar promotes the idea of data stewardship and the importance of updating software and hardware security protocols by highlighting the role of vendors.

d. *Pillar Four:* Invest in a Resilient Future. Another vital aspect of the NCS is its concept of investing in the future of cyberspace. This can be seen in the commitment to initiate strategic investments in innovation, R&D, and education. This is to ensure the country's leadership in cyberspace and thwart the advantages of its adversaries.

e. *Pillar Five:* Forge International Partnerships. This last pillar states the commitment of the US to maintain the free and open nature of cyberspace while ensuring its security. This can be done through global regimes that countries can adhere to. For this reason, the NCS underscores the need for the US to engage with like-minded nations and organizations to foster practices and forge agreements that will promote shared values. This pillar is also concerned with assisting partners and allies to enhance their cybersecurity capabilities.

The Five Pillars of the US National Cybersecurity Strategy

Figure 13


Defend critical infrastructure
Disrupt and dismantle threat actors
Shape market forces to drive security and resiliency
Invest in a resilient future
Forge international partnerships

Source: White House, 2023

What can we learn from these experiences and related works?

Attaining a cyber defense posture can be a daunting task for a small country like the Philippines. However, we need to learn from the experiences of our allies and partners to be able to maximize our resources for this effort. Table 2 shows the summary of the cyber strategies of the abovementioned countries.

Summary of Cyber Strategies

Table 3

National Cyber Strategies	Notable Points	General Summary & Lessons
Canada	• Emphasizes the importance of defending critical infrastructure and resilience. • Highlights the need for leadership and collaboration with the private sector. • Addresses the skills and capacity gaps. • Stresses the role of institutions.	The following are the lessons that can be derived from the 3 country examples: • There is a recognition that cyberspace is a vital component of national development and security. • All cases cited the need to secure its critical infrastructure and ensure resilience. • To be competitive, there is a need to develop standards and talent. • There is a need to understand threat actors and forge partnerships to mitigate these threats. • Institutional building is a key component of a robust cyber defense.
United Kingdom	• States that cyber power is a component of national power, thus the need for the country to ensure its leadership in cyberspace. • Emphasizes the need to protect its digital ecosystem and ensure its resilience. • “Defend as one”- stresses the collaborative nature of cyber defense. • Points to the need to adopt active cyber posture against its adversaries.	
United States	• Highlights the importance of defending critical infrastructure and fostering resilience. • Adopts the idea of forward defense which focuses on preparedness, resilience, and the ability to mitigate/disrupt the sources of cyber threats. • Shifts in cyber strategy thinking: Rebalancing of roles and strategic investments.	

Source: Annotations by the Author

a. *Cyberspace is a component of national development* - In all country strategies, there is a common understanding that cyberspace is a venue for innovation, growth, and freedom. Because of the ubiquitous nature of its digital ecosystem, these countries envision that cyberspace plays an important role in harnessing the potential of emerging technologies like artificial intelligence and quantum computing, among others.

b. *Defending critical infrastructure and ensuring resilience is a must* - The national development view comes with the need to defend critical infrastructure against malicious attacks. The strategies underscore the need to ensure citizens’ privacy and provide access to reliable information as well as online services. The plans focus on increasing the ability of the public sector at all levels (federal and local) to defend its systems and data. Furthermore, these plans recognize the need for collaborative action that includes the private sector and these countries’ citizens.

c. *Standards and resources must be developed* - The country strategies mentioned the need for developing a common standard for cybersecurity as well as the importance of investing in vital resources. Standards like the ISO 2007, and NIST 800x among others are models that can provide regulatory guidelines for states. Furthermore, these standards can also serve as roadmaps on how to achieve cyber defense goals.

d. *Forging partnerships, building institutions, and mitigating threats are crucial* - Finally, the plans underscore the importance of building international and local partnerships, thus the emphasis on collective defense or actions in protecting cyberspace. Moreover, the experiences of these countries also reveal the need to empower existing law enforcement and security agencies as well as to legislate new laws to achieve their goals.

Framework for Attaining a Cyber Defense Posture

Table 4

Attaining a Cyber Defense Posture		
General Summary and Lessons from Canada, the UK, and the US	**Passive Cyber Defensive (PCD)**	**Active Cyber Defense (ACD)**
Recognize cyberspace as venue for national development	For both PCD and ACD, it is crucial for policy makers and security planners to consider the importance of cyberspace in national development as well as the security aspect of a country's digital ecosystem. Also adopting a citizen-centric approach will be useful	
Defend critical infrastructure	• Identify a country's critical infrastructure together with its stakeholders. • Identify its vulnerabilities and risks. • Develop an action plan on how to protect it. • Adopt continuity and resiliency practices.	• Attacks on its critical infrastructure can be mitigated through economic sanctions and other political/diplomatic means. • States can develop capabilities to retaliate against these attacks. This can be done through kinetic or cyberattacks or both.
Develop standards and resources	• Adopt a common standard that will identify phases and activities. • Address the competency gaps in cyber. • Ensure a timely response to cyber-attacks. • Aid the private sector about their cybersecurity issues.	• Build a cyber force that can pursue offensive operations. • Develop the ability to "hack back".
Forge partnerships, build institutions, and mitigate threats	• Adopt a collective paradigm with government and its partners as well as the private sector for a secure cyberspace. • Build the capacity of law enforcement, security, and other civilian institutions to ensure its resilience. • Adopt practices like information/intelligence sharing and threat assessments on the vulnerability of various sectors of society. • Provide early warning and incident notification. • Adopt honey pot techniques to determine attack morphology. • Forge agreements with like-minded states and partners on the sharing of best practices and information.	• Pursue proactive activities like profiling, active surveillance, and cooperation with allies and partners concerning an emerging cyber threat. • Adopt "honey pot" techniques designed to observe attack morphology. The purpose of this is to emulate these techniques for offensive intent.

Source: Annotations by the Author

Attaining a Cyber Defense Posture

To attain a credible CDP, its proponents must understand that the main reason for this shift in thinking is to protect Filipinos from disruption, anxiety, and fraud in cyberspace. This citizen-centric view also underscores the need to protect the country's digital ecosystem. To do this, the Philippines can examine the country strategies and combine them with the concept of passive-active cyber defense. Table 3 presents the result of this combination, thus providing a starting point for defining the country's cyber defense posture.

Implications for the Philippines

Current geopolitical tensions and the ensuing competitive environment place the Philippines at a crossroads in terms of securing its interests in cyberspace. The country's digital transformation agenda requires a secure digital ecosystem that can foster trust as well as ensure reliable access to information and services. Furthermore, the country's security alliances make it a likely target for malicious cyber-attacks and other influence operations. This underscores the importance of adopting a cyber defense posture that will serve as a framework for the collective defense of our society. For this, the following recommendations are put forth:

a. Form a Technical Working Group on Cyber Defense (TWG-CD)

The task of the TWG-CD is to work on the initial cyber defense framework discussed in this paper. To adopt a collective defense paradigm, the TWG-CD is envisioned to include representatives from the public and private sectors. Members of the group shall be tasked to further examine the concept of cyber defense and its various aspects. The group should identify the laws and harmonize the various plans and continuity templates and recommend how the CDP can be integrated into the upcoming national security, digital transformation, and cyber security strategy of the Philippines. Furthermore, an executive order can be promulgated designating the National Security Council (NSC) to have direct oversight over the TWG-CD. The DICT, DOJ, DILG, DTI, NICA, and the DND are possible members of the TWG. Enumerated below are the major outputs for the TWG:

i. *Initiate a survey of critical sectors and their vulnerabilities* - Part of the TWG's task is to come up with an initial list of critical sectors. The Office of the President through the NSC should ask the concerned national agencies to determine its critical sectors and services. Line departments that can be mobilized for this task are as follows:

Departments of Defense, Interior Interior and Local Government, Energy, Agriculture, Trade and Industry,Transportation, and Finance.

ii. *Develop an action plan to implement the CDP* - The TWG-CD is expected to propose an action plan that will ensure that the CDP and its resulting strategies can be implemented and sustained. For this, the group can identify laws, propose the creation of new agencies, and design programs as well as incentives that can encourage the participation of public agencies together with the private sector.

iii. *Develop a cyber maturity tool* - The TWG can initiate the creation of a cyber maturity tool that will provide a baseline measure of cybersecurity in the various sectors. This tool can include measures on the following: (a) Policy and Structure (b) Cyber Security Standards (c) Technical Infrastructure and (d) Human Resources.

iv. *Map Competencies* - Another crucial aspect of the TWG's role is to identify the competencies needed to adopt and sustain a CDP. This will guide organizations in strengthening their human capacities and fostering resilience.

b. Increase Cooperation with International Partners and Allies

Defending alone will ultimately lead to failure. The Philippines must harness the collective experience of its international partners and allies. Aside from the three countries cited in this paper, the experiences of Australia and Singapore are excellent references.

c. Incorporate CDP into the Cyber Plans of Critical Sectors

Recognizing the value of collective cyber defense is crucial for a whole-of-society approach. Policymakers, planners, and advocates should avoid seeing the country's cyber strategy as a function of individual departments and organizations. A CDP should encourage actors to view the responsibility of securing cyberspace as a mosaic where each plays a part in achieving its goals.

references

60 Minutes. (2022). China's Cyber Assualt on Taiwan. Retrieved from https://www.youtube.com/watch?v=Agc3vy-JD4c

Addington, D., & Manrod, M. (2019). Cyber security threats and solutions for the private sector. In M. Gueldry, G. Gokcek, & L. Hebron, Understanding New Security Threats (pp. 181-195). New York: Routledge.

Argosino, F. (2023). P155 M lost to over 8,000 online scams from January – August 2023 . Retrieved from Inquirer.net: https://newsinfo.inquirer.net/1833108/over-8000-cases-of-various-scamming-schemes-logged-from-january-to-august-2023-pnp

Bangko Sentral ng Pilipinas. (2023). 2022 Status of Digital Payments. Bangko Sentral ng Pilipinas.

Canada Center for Cyber Security. (2022). National Cyber Threat Assessment. Ontawwa: Communications Security Establishment.

Curtis, J. (2021). Springing the 'Tacitus Trap': countering Chinese state-sponsored disinformation. SMALL WARS & INSURGENCIES, 229-265.

Denning, D. (2014). Framework and principles for active cyber. Computers and Society, 108-113.

Denning, D. (2014). Framework and principles for active cyber defense. Computers & Security, 108-113.

Duffy, K. (2022, April 22). A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine. Retrieved from Business Insider: https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4

Ene, C. (2023). 10.5 Trillion Reasons Why We Need a United Response to Cyber Risk. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=6f9eb7063b0c

Fanelli, R. (2016). Cyber Defense and Offense. Journal of Information Warfare, 53-65.

Friedrich Naumann Foundation. (2020). The Philippine Government's Losing War on Disinformation. Retrieved from Friedrich Naumann Foundation: https://www.freiheit.org/philippines/philippine-governments-losing-war-disinformation

Gandhi, H. (2019). ACTIVE CYBER DEFENSE CERTAINTY: A DIGITAL SELF DEFENSE IN THE AGE OF MODERNITY. Oklahoma Law Review, 101-131.

Goldman, E. (2022, Winter). Paradigm Change Requires Persistence-A Difficult Lesson to Learn. The Cyber Defense Review, pp. 113-120.

Goldman, E., & Warner, M. (2021). The Military Instrument in Cyber Strategy. SAIS Review of Intenrational Affairs, 51-60.

Government of Canada. (2018). National Cyber Security Strategy. Ottawa: Public Safety Canada.

Government of Canada. (2019). National Cyber Security Action Plan 2019-2024.

HM Government. (2022). National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK. London.

HM Government. (n.d.). Government Cyber Security Strategy: Building a cyber resilient public sector 2022-2030. London: Cabinet Office.

Hon-min, Y. (2019). A critical strategy for Taiwan's cybersecurity: a perspective from critical security studies. Journal of Cyber Policy, 35-55.

Howe, S. (2023). Social Media Statistics in the Philippines. Retrieved from Meltwater: https://www.meltwater.com/en/blog/social-media-statistics-philippines

Hsini, H., & Tien-Shen, L. (2018). A centralised cybersecurity strategy for Taiwan. Journal of Cyber Policy, 344-362.

International Telecommunications Union. (2022). Fixed broadband subscriptions (per 100 people) – Philippines. . Retrieved from World Bank Database: https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=PH

International Telecommunications Union. (2022). Individuals using the internet (% of population) – Philippines. Retrieved from World Bank Database: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021 &locations=PH&start=2001&view=chart

International Telecommunications Union. (2022). Mobile cellular subscriptions (per 100 people) – Philippines. Retrieved from World Bank Database: https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=PH

International Telecommunications Union. (2023). Global Cybersecurity Index 2020. Retrieved from ITU Publications: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Lucas, D. (2021, September 3). Diokno to PH fintech firms: 'Strike while the iron is hot'. Retrieved from Inquirer.Net-Business: https://business.inquirer.net/330039/diokno-to-ph-fintech-firms-strike-while-the-iron-is-hot

Manantan, J. (2020). The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the SCS. Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs, 1-29.

Occeñola, P. (2019). Exclusive: PH was Cambridge Analytica's 'petri dish' – whistleblower. Retrieved from Rappler: https://www.rappler.com/technology/social-media/239606-

ODB. (2020). Open Data Barometer-East Asia and the Pacific. Retrieved from Jakarta Labs, World Wide Web Foundation: https://opendatabarometer.org/4thedition/regional-snapshot/east-asia-pacific/#country-profiles

Ronda, R. A. (2023). Philippines 2nd most attacked by web threats worldwide last year. Retrieved from Philstar: https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 154-176.

SWS. (2020, September 8). Fourth Quarter 2019 Social Weather Survey Special Report: 45% of adult Filipinos are Internet users. Retrieved from Social Weather Stations: https://www.sws.org.ph/swsmain/artcldisppage/?artcsyscode=ART-20200908150946&mc_cid=6e4c1b81d9&mc_eid=31b9d30a85

United Nations Department of Economic and Social Affairs. (2022). UN E-Government Knowledgebase - Philippines. Retrieved from United Nations Department of Economic and Social Affairs: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/134-Philippines/dataYear/2022

White House. (2018). The National Cyber Strategy of the United States of America. Washington, D.C.: US Government.

White House. (2023). National Cybersecurity Strategy . Washington, D.C.: United States Government.

Whyte, C., & Mazanec, B. (2019). Understanding Cyber Warfare: Politics, Policy and Strategy. New York: Routledge.

www.stratbase.ph

SPARK®
the key link between IDEAS and ACTION

The Financial Tower,
6794 Ayala Avenue,
Makati City 1226

V (632) 7000.2748
F (632) 7005.3779

stratbase

+ ADRi
ALBERT DEL ROSARIO INSTITUTE
FOR STRATEGIC AND INTERNATIONAL STUDIES

SPARK

The key link to idea and action – is the on-line newsletter of ADRi (Albert Del Rosario Institute) that covers socio-political, economic and security analysis of timely issues that affect the direction of the economy and political landscape governing the Philippines.

STRATBASE ADR INSTITUTE

Stratbase ADR Institute is an independent, international and strategic research organization with the principal goal of addressing the issues affecting the Philippines and East Asia through:

1) effecting national, regional and international policy change or support;

2) fostering strategic ideas based on cooperation and innovative thinking;

3) providing a regional venue for collaboration and cooperation in dealing with critical issues in East Asia; and

4) actively participating in regional debates and global conversations.