CYBERSECURITY IN THE PHILIPPINES:

GLOBAL CONTEXT AND LOCAL CHALLENGES

a report by Secure Connections
an initiative of The Asia Foundation

Secure Connections

The Asia Foundation

CYBERSECURITY IN THE PHILIPPINES:
GLOBAL CONTEXT AND LOCAL CHALLENGES

a report by Secure Connections
an initiative of The Asia Foundation

March 2022

ABOUT THE PARTNERS

Secure Connections

Secure Connections is a coalition of stakeholders that aims to bring together knowledge and expertise from the public, private, and civil society sectors for the improvement of Philippine cybersecurity. Secure Connections is supported by The Asia Foundation – Philippines.

The Asia Foundation

The Asia Foundation is a nonprofit international development organization committed to improving lives across a dynamic and developing Asia. Informed by six decades of experience and deep local expertise, our work across the region addresses five overarching goals—strengthen governance, empower women, expand economic opportunity, increase environmental resilience, and promote regional cooperation.

ACKNOWLEDGMENTS

This report was prepared by members of Secure Connections, namely Angel S. Averia, Jr.; Gamaliel Pascual; William Emmanuel Yu, Ph.D.; Mary Grace Mirandilla-Santos; Angelo Niño Gutierrez; Bas Claudio; Dan Mejes; and Froland Tajale.

Kim Pobre, Jestine Mendoza, Ferth Manaysay, and Ranna Pintor also contributed to this report.

The authors are grateful to Jaime Faustino and Sam Chittick for their invaluable contribution in refining ideas and recommendations. They also thank Oliver Xavier Reyes for his insight and expertise, and Ritchelle Buensuceso and Mariel de Jesus† for copyediting the report.

The authors are responsible for the content and views expressed herein. These views should not be attributed to The Asia Foundation, whose support for this publication is gratefully acknowledged.

FOREWORD

Advancements in digital technologies have altered many aspects of Philippine society. The impressive economic growth from 2010–2020 was parallel to tremendous advances in digital technologies, opening opportunities in new sectors. The opportunities from digital innovations were accelerated by the COVID-19 pandemic as limitations on mobility prompted citizens to accelerate migration to digital spaces. These changes can be seen in the growth of digital payment systems, online meeting platforms, electronic health services, online retail, direct delivery services, and many others.

However, with increasing connectivity comes increasing cyber threats. Individually, Filipinos are susceptible to data breaches and privacy violations online. On a societal level, cyberattacks by state or nonstate actors on critical infrastructure can undermine national security and impact economic activity. While cyber threats originate online, their consequences can manifest beyond the digital space into our physical lives.

These kinds of attacks also have direct economic costs. Firms spend more to repair infrastructure damaged by ransomware attacks. A 2018 study by Frost & Sullivan found that potential economic loss in the Philippines due to cyberattacks can reach USD 3.5 billion or 1.1% of the total Philippine GDP.

To address these challenges, Secure Connections—a coalition of cybersecurity advocates organized by The Asia Foundation—has produced this report on the state of cybersecurity governance in the Philippines. The report draws on extensive research to further the goals outlined in the National Cybersecurity Plan of 2022 of increasing the nation's cyber resiliency, protecting critical infrastructure, and promoting greater cyber awareness. The report traces the shifts in Internet governance and features the cybersecurity policy and posture of select countries and their possible implications on the Philippines' own cybersecurity position. We offer this examination of cybersecurity institutions at the global, regional, and national levels as a crucial contribution in improving our understanding, and crafting, of the Philippines' cybersecurity posture.

We hope this report contributes in exchanging ideas and building our collective knowledge on how to make digital spaces safer and more secure. We offer an analysis for this point in time of the evolving cybersecurity threats, current and potential issues, and concrete steps to address them. If we can set the foundations for improved cybersecurity governance, we will all help the future security and prosperity of the country.

Sam Chittick
Philippines Country Representative
The Asia Foundation

TABLE OF CONTENTS

Key Messages 10

Introduction 11

PART 1: INTERNET, CYBERSECURITY, AND GLOBAL CONTEXT **15**

Chapter 1: Opportunities and Risks in a Newly Digitalized World **17**

Risks Affecting the Digital Shift 17

Malicious Cybersecurity Attacks 21

The Reenergized Need for Cybersecurity 22

Chapter 2: The Internet-Enabled New World Order **28**

A Brief History of the Internet 28

The Fragmentation of the Internet 30

A Brief History of Cybersecurity 36

Chapter 3: Regional and National Cybersecurity Frameworks **41**

International and Regional Frameworks 41

Elements Behind National Strategies and Frameworks 43

Cybersecurity Governance Frameworks of Select Nations 49

Australia 50

China 56

Israel 59

Russia 63

United States 66

Indonesia 71

PART 2: PHILIPPINE CYBERSECURITY ISSUES AND CHALLENGES 79

Chapter 4: State of Philippine Cybersecurity: Critical Infrastructure and Key Sectors **80**

Critical Infrastructure 80

Electronic Government 86

Electronic Commerce 92

Electronic Banking and Financial Services 95

Healthcare Management 99

Energy Resources Management 104

Water Resource Management 109

Transportation 113

Telecommunications and Internet 117

National ID System 122

Automated Election System 133

Education 140

Working from Home 145

Chapter 5: Findings and Recommendations for Improving Cybersecurity in the Philippines 160

Glossary 168

Images / Photos Credits 178

References 181

LIST OF TABLES & FIGURES

Table 1. Common Threads in National Security Frameworks of Select Countries 48

Table 2. Critical Infrastructure Sectors in Select Countries 83

Table 3. Examples of CI Institutions in Select Sectors 84

Table 4. Demographic Data and Biometric Information Collection under the PhilSys Act 123

Table 5. Comparative Details of RMA Results, 2010–2019 National and Local Elections 138

Table 6. Global Cybersecurity Index Score and Ranking of Select Countries 153

Table 7. National Cybersecurity Index Score and Ranking of Select Countries 155

Figure 1. Australian Government's Cybersecurity Arrangements 51

Figure 2. BSSN Synergizes the Elements of National Security 73

KEY MESSAGES

- The pace of digitalization, defined as the use of digital technologies that are fundamentally changing processes, creating new business models and significant social change, has only increased with the pandemic. With the rapid growth of the digital ecosystem comes a significant increase in cybersecurity risks.

- In the Philippines, cybersecurity is not seen as a priority yet. Because the country is still at the initial stage of digital transformation, there seems to be a misconception that threat actors do not pose as serious a threat or that the Philippines is not a target.

- Cybersecurity needs to be a key priority of the Philippines if it intends to participate more meaningfully in, and benefit from, the fast-growing global digital economy.

- Drawing on lessons from the proven practices of Australia, China, Israel, Russia, and the United States while acknowledging the distinguishing characteristics of the Philippine context, this report concludes with a set of recommendations focused on cybersecurity knowledge, policy, and skills gaps in order to improve the Philippines' cybersecurity posture:

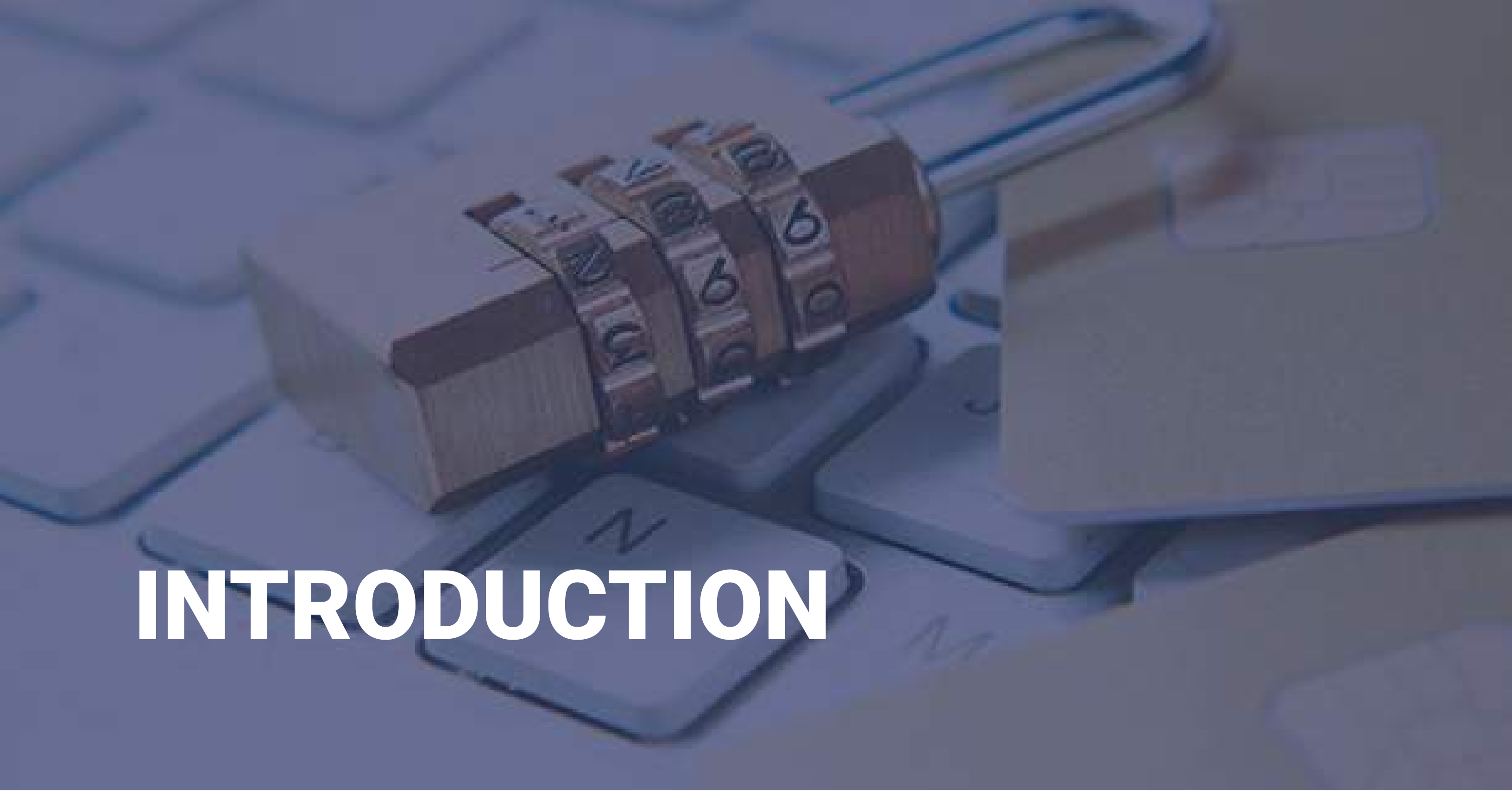
    1. Create **greater awareness of the global and local cybersecurity context** and a better appreciation of the threat landscape.

    2. Generate and analyze **local data on cybersecurity practices and incidents** on a sectoral level in order to identify security gaps, inform decisions and policy, and provide appropriate solutions.

    3. Adopt **minimum information security standards** for all public institutions and encourage compliance with well-established and internationally accepted frameworks, especially for critical infrastructure.

    4. Develop a **cybersecurity culture** by raising awareness, supporting training and capacity building for cybersecurity talent, and instilling cybersecurity as a way of life through educational institutions.

    5. Nurture an environment of **cooperation and information sharing** among the local and international cybersecurity communities because an incident for one can be a lesson for another.



INTRODUCTION

The 21st century has seen a steady increase in the availability of different online services catering to the whole range of human activity, from wake to sleep. The ubiquity of these technology-enabled tools has increased pressure on the public and private sectors, on people and businesses, to embrace the transition to digital. This accelerated growth has also increased cybersecurity[1] threats. Daily there are news reports on attacks on critical infrastructure[2] such as banks and pipelines; high-profile personalities, including public officials; and online platforms like social media. And given the rapidly changing socio-political and economic environment, advancements in technology, and evolving business models such as the franchisification[3] of malware and the emergence of malware-as-a-service, cyber risks are expected to increase in number and sophistication.

Impact of digitalization

Any previous perception that the digital universe is but a luxury limited to the privileged has been eroded by the COVID-19 pandemic, particularly in 2020 through 2021.

Early 2020 marked a significant change in everything people, businesses, and governments do on a global scale due to the COVID-19 pandemic. Many enterprises were forced to enable online digital workspaces that allowed more of their employees to work from home. Working from home leverages digital technology to move business operations online, with employees clocking in virtually and businesses providing access to their internal networks using virtual private networks or similar solutions over the public Internet. Employees and employers alike, working from their homes, might have welcomed the elimination of their daily commute but were confronted with the need to compete for bandwidth[4] with their children, who themselves were studying from home through remote learning.[5] Workers who might have relied on takeouts or leisurely lunch breaks at the nearest mall now either cooked their own lunches or had them delivered using online apps. This created a market boom for online delivery services, even prompting some companies to pivot and cater to this new demand. An example of such is Grab, who has been forced to shift its focus from ride sharing to online delivery. Payments for deliveries are often through digital wallets replenished by online banking—after all, one did not want to risk getting infected with COVID-19 by lining up for groceries or stepping inside a bank.

Commerce has also shifted online as the drop in physical retail has forced companies to remodel their operations. Small and large businesses have increasingly relied on websites, social media, and chat apps not only to promote their brands to customers but also to accept orders and online payments for goods and services. Thus, there has been a considerable increase in mobile wallet registrations and online and mobile banking transactions, with the Bangko Sentral ng Pilipinas, the country's central bank, reporting that 17% of all payment transactions in the first half of 2020 were digital payments (Chipiongian, 2021).

Another key area affected by digitalization[6] is education. With schools as potential hotspots of infection, multiple governments decided to defer in-person classes until a vaccine becomes available. This leaves students with remote learning, ideally from home, as the only option for continuing their education during the pandemic. Remote learning, especially at the tertiary level, has offered more options for further education particularly for those already working. Through remote learning, those interested in earning master's degrees from prestigious foreign universities could even do so without disrupting their lives by having to relocate overseas.

Cybersecurity as a critical issue

This rapid growth in digital activities has also increased cybersecurity threats, particularly for critical infrastructure. Over the past several years, the world has witnessed more and more cyber incidents involving key sectors such as water, power, and telecommunications that are vital to life and maintaining societal functions. Disruption to these critical infrastructures is also fast becoming a weapon for cyberwarfare against rival states. Hence, the protection of critical infrastructure against cyberattacks[7] must be a primary goal of every country.

The pandemic highlighted how malicious actors will take advantage of every opportunity, especially a crisis, when people are most desperate and vulnerable, to launch cyberattacks. The shared experience of various countries in dealing with the COVID-19 pandemic and the concomitant cybersecurity challenges that it brings can be a valuable source of learnings moving forward.

A country's cybersecurity posture can have a huge impact on its national security, economy, access to technology and innovation, and foreign policy. Cyber capability and readiness to identify and respond to incidents are crucial to protecting and sustaining the delivery of essential services to people. Cybersecurity policies and strategies can determine the entry of foreign investment and the participation of citizens in the global digital economy. Therefore, nations should protect and promote cybersecurity in order to reach its full digital potential

This report is a contribution to the critical discussion of cybersecurity in the Philippines. Part 1 of the report outlines the broad global context, the evolving cybersecurity risks and challenges that come with digitalization, and various efforts to develop regional and national cybersecurity governance frameworks. Part 2 focuses on key sectoral cybersecurity challenges for the Philippines and concludes with findings and recommendations on how to improve the country's cybersecurity posture in an environment of rapid change and increased threats.

Endnotes

[1] The state of having secure data, systems, networks, and other information and communications technology (ICT) assets, protecting them from malicious attacks and any other threats to their integrity (National Institute of Standards and Technology, 2015).

[2] Assets, systems, and networks, whether physical or virtual, that are considered so vital that their destruction or disruption would have a debilitating impact on national security, health and safety, or economic well-being of citizens, or any combination thereof (Migration and Home Affairs, n.d.). Examples include the banking system, oil pipelines, water systems, and electricity systems.

[3] “Franchisification” means to operate using a franchising business model, which is now being used to carry out cyberattacks. An investigation by Trend Micro in 2021 found that some malicious actors rebrand a “supplier” of ransomware before they are deployed (Merces, 2021).

[4] “Bandwidth” refers to the speed or amount of data that can be transferred over an Internet connection. For more information on bandwidth and broadband in general, see World Bank (2012).

[5] The practice of conducting classes and other traditionally school-bound activities from a distance, using a mix of ICT and traditional technologies such as printed modules (Butcher et al., 2015). Also known as distance learning.

[6] The shift of content, processes, operations, and activities to computer- and/or Internet-enabled forms. Also used to describe the work of transforming objects and assets from the physical world into digital form to take advantage of ICT’s transformative potential for business or activity models (IBM, n.d.-b).

[7] Any malicious activity aimed at stealing, manipulating, disabling, or otherwise disrupting a network, system, or information in a targeted manner (National Institute of Standards and Technology, 2012).

PART 1:

Internet, Cybersecurity, and Global Context

The Internet has transformed the way people live, how organizations operate, and the pace at which countries develop and thrive. Virtually connecting people anywhere in the world has made remote work, distance learning, e-commerce, telemedicine, and online banking, among others, possible. This has created a huge opportunity for nations to take a new development path. Countries that took advantage of technology, especially the Internet, have leapfrogged development. Global superpowers are now defined by how much they are able to harness the power of technology. Meanwhile, nations that are not equipped to use technology are lagging behind.

The pervasiveness of the Internet has created the digital economy, where every link in the value chain is mostly driven by digital platforms. The shift from digitization—the process of converting analog to digital formats (IBM, n.d.-b)—to digitalization—the use of digital tools to change business processes that can result in new business models and social change—has led to a transformation unlike anything the world has seen before. This digital transformation was further accelerated by the COVID-19 pandemic, which forced the whole world to impose lockdown restrictions and conduct everyday activities remotely.

With this digital shift comes a wide range of cybersecurity risks. As Internet technologies advance, so do cybersecurity threats and modes of attacks. Cybersecurity protection is no longer just nice to have; it has become a necessity for every nation, organization, and individual. Because of the fast pace of digitalization, there is little doubt that cybersecurity and economic development are intimately related. Thus, cybersecurity governance, which defines how regions and nations ensure the protection of information, information and communications technology (ICT) systems and networks, and digital assets (Bodeau et al., 2010), must now be considered a priority.

Part 1 provides the global context of the Internet and cybersecurity and how these may impact countries like the Philippines.

Chapter 1 gives an overview of the opportunities and risks brought about by a newly digitalized world. It explores the scale and depth of the sudden digital shift because of the pandemic—from work-from-home arrangements, e-commerce, digital banking, to online learning—and related cybersecurity attacks.

Chapter 2 deep-dives into how the Internet changed the world order. It shows the relationship between the twin evolution of the Internet and cybersecurity issues. This chapter also discusses the splintering of the Internet, which reflects how different countries view the Internet and respond to cybersecurity issues.

Chapter 3 discusses the key features of the existing and emerging regional and national cybersecurity governance frameworks, with a special focus on select Asia Pacific countries, Australia, China, Israel, Russia, and the United States.

1 | Opportunities and Risks in a Newly Digitalized World

> “The sudden digital shifts occasioned by the pandemic have been exploited by malicious actors, particularly through the deployment of cyberattacks.

In this world of “everything from home,” digitalization has increased the risks for different forms of cyberattacks. Vulnerabilities in the systems of online platforms provide opportunities to target individual users, organizations, and institutions. Data leakages[1]/ransomware (Chuan, 2020) and e-commerce[2] fraud (Cayon, 2020) are just some of the digital crimes that have increased during the pandemic. These online risks may not be sufficient to deter the demand for the digital shift. However, the pressure to transition without a sufficient understanding of the dangers involved decreases the opportunities to mitigate those risks, endangering those who are supposed to be empowered and benefitted by the next phase in the digital age.

Risks Affecting the Digital Shift

Work from Home

Working remotely entails connecting an internal network to the public Internet in order to provide access to business services and resources, opening the proverbial Pandora’s box. Two of the most common ways to work from home[3] are (1) using a cloud service provider[4] to host the organization’s network or (2) facilitating access to the internal network from the Internet using a virtual private network (VPN).[5] The choice boils down to either “put what we have outside” or “let people in.” In both scenarios, the traditional “digital castle” mentality of defending around a handful of protected networks where people would work has eroded. Where, after all, within the digital realm is outside and inside?

The integrity of all parts of the network is paramount to ensuring the security of sensitive business data and services, whatever the method used to provide remote access. Modern cryptography[6] and virtualization technology[7] have made the options quite secure and accessible; it is ultimately good practice to apply both technologies. Unfortunately, work-from-home (WFH) arrangements render the employment of either cryptography or virtualization more difficult due to the complexity of managing the security for tens, hundreds, or even thousands of employees remotely.

In more measured times, most organizations can steadily roll out their secure networks that adequately protect their systems and data despite the increased security risks with WFH. But in 2020, with the pandemic and mobility restrictions, many organizations only had a few days to enable the shift.[8] The experience has forced organizations to rethink how they protect their assets, compelling them to shift focus from protecting networks to protecting assets instead. Yet this assumes that all connections can come from either protected or unprotected networks whether in the office or at home. This has given birth to new paradigms such as zero trust network architecture,[9] where every connection must be properly identified and authorized irrespective of its underlying network.

Secure WFH arrangements are further complicated by the risks of Bring Your Own Device (BYOD) practices—that is, allowing employees to use their personal devices to access the organization's network and other information technology resources instead of issuing dedicated work devices to employees (Citrix, n.d.). Organizations that did not, or could not, issue their employees such dedicated devices as phones, tablets, and personal computers before the lockdown now have no choice but to implement BYOD.

Unfortunately, personal devices are often lacking in security, due to a combination of poor security awareness and risky online behavior from users. Personal computers often have outdated antivirus[10] software and may also be used to download illicit and often malware-ridden[11] content from the Internet, such as pirated software. Smartphones may contain questionable apps or be used to visit compromised websites. As more valuable corporate information is placed in the hands of these consumer systems, it has become a lucrative target for potential bad actors focused on the ransomware trade. Ransomware is a subtype of malware that hijacks systems and prevents access to a part or all of an organization's data, unless a ransom is paid to the criminal group behind the ransomware (Fruhlinger, 2020a). To further push victims to pay up, threat actors may also leak information if the ransom is not paid.[12] Organizations now must protect information in a larger range of devices. The need to improve security measures associated with BYOD policies becomes more important.

E-commerce and Digital Banking

E-commerce and ecosystem providers are seeing brisk business during the pandemic. The proliferation of person-to-person (P2P) business transactions (i.e., individual traders in open marketplaces) has already driven the usage of peer-to-peer money transfers.[13] These changes have led to an increased dependence on financial technology, as summarized by a Philippine bank industry veteran:

> During the COVID-19 crisis, the volume of over-the-counter branch transactions dropped to half. On the other hand, digital payments, in various forms, soared exponentially—between three and eight times. It is difficult to imagine payments to go back to manual after the [COVID-19] crisis is over. Once banking customers taste the convenience of mobile banking, they will stay mobile (Acevedo, E. personal communication, May 9, 2020).

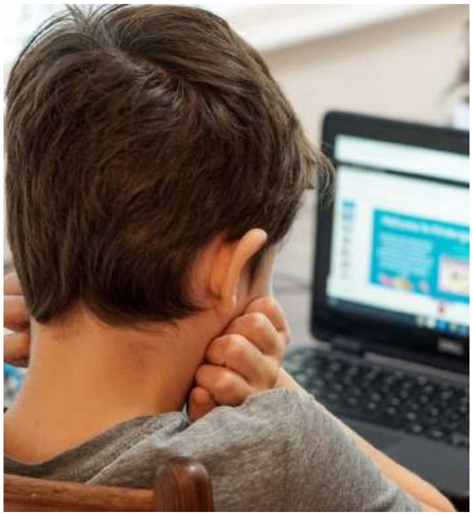
The amount of data processed and recorded on digital platforms increases with the surge of customers. This makes these platforms increasingly lucrative targets for bad actors, with cybercriminals targeting both retailers and consumers. Cyber threats such as business email compromise,[14] phishing,[15] ransomware, e-commerce data interception, cyber scams, cryptojacking,[16] and crimeware-as-a-service[17] have been identified by the International Criminal Police Organization (Interpol) in 2021 as the top cyber threats in Southeast Asia (Interpol, 2021). With more businesses now online and more customers shopping online, the interest is in harvesting customers' personal identifiable information and payment card details that retailer sites collect and store. Such personally identifying information is used to hijack personal accounts, hold it for ransom, or sell it on the dark web.[18] Indeed, criminal enterprises such as installing ransomware and threatening to leak data have emerged as growing businesses in themselves.

Online security risks are magnified in the e-commerce space due to the increased acquisition by many businesses of third-party services such as cloud services or VPN providers,[19] which ostensibly facilitate secure online transactions or WFH environments. Securing assets in the cloud is difficult, as evidenced by the major breaches[20] in large companies like Capital One Financial Corporation[21] as well as in smaller organizations. Ideally, the onus of cloud security[22] is on both the cloud provider and the customer, under a model of shared responsibility. Yet, not all cloud users are themselves properly versed in securing themselves or their data in the cloud, and such necessary capacity may not have been built prior to the shift to cloud services.

Moreover, the sudden need to transition brought about by the pandemic may have pressured enterprises to quickly obtain cloud services without exercising due diligence to ensure against service providers with haphazard services that ultimately compromise the organization's security. Numerous examples exist of disreputable service providers compromising their clients' security, leading to data leaks or interrupted operations. In one case, VPNs that promised not to log their customers' activities—an important security feature for business and individual users alike—not only logged but also leaked data through poor security practices (Kan, 2020). Similarly, cloud providers that fail to adequately secure user credentials can lead to attackers gaining access to business data and services (Cimpanu, 2020a). Issues are not only limited to disreputable providers. Even the most reputable of providers are subject to cyberattacks. Due diligence is necessary, but appropriate controls must also be put in place to limit the resulting damage should a cyberattack gain access to a computer system.

Online Learning

Just as education technology (EdTech)[23] has existed before the pandemic, so have the privacy and security risks that come with giving young students access to resources on the Internet. Online platforms often collect sensitive information from students, in addition to potentially sensitive data[24] such as photos and videos. Improperly secured, this information could fall into the wrong hands and be used for identity theft and other similar crimes (Muncaster, 2018). For younger children who may be less conscious about leaving their cameras and microphones on when not in use, this is a major concern. In one instance, for example, a cybercriminal group stole data from EdTech platforms and used children's information in various extortion schemes against the students' parents (Sullivan, 2019). The use of social media, in particular, can inadvertently expose data (including photos) of minors without proper consent.



EdTech is covered by the relevant laws on data protection, such as the European Union's General Data Protection Regulation and the Philippine Data Privacy Act (Common Sense, 2019). This alone, however, is no assurance that any given platform will keep data secure. In 2019, for example, a study found that 80% of the most popular EdTech failed to meet adequate levels of privacy protection, despite the existence of regulations (Common Sense, 2019). The major reason is the *analog gap*. Content and information are secured in these centrally managed platforms, which are normally suitably protected. However, when a student or teacher produces or consumes content, it still has to be rendered on a screen, played back on speakers, or downloaded into a device. The digital information leaves the protection of the centrally managed and secured platforms. This content or information, converted from digital to analog in order to be perceived by humans, is what can be stolen or exploited.

What makes EdTech particularly risky is that it is designed to be used by children and young people—a demographic that is unlikely to be fully aware of risks online. Children are less likely to identify threats, such as compromised links, phishing attempts, and malware, leaving them vulnerable to attacks from malicious actors.[25] Similarly, young people are less likely to discern what information they should and should not share online, which can be exploited by criminals in various schemes.

Malicious Cybersecurity Attacks

The sudden digital shifts occasioned by the pandemic have been exploited by malicious actors, particularly through the deployment of cyberattacks. An Interpol study used data from 194 member countries to assess the rise in cyber-related crimes during the pandemic. They found that 907,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs—all related to COVID-19—were detected in one four-month period from January to April of 2020 (Interpol, 2020b).

These malicious actors have employed several types of attacks to fulfill their objectives, which include the following:

Malware. Malicious software is usually located in fake websites that appear legitimate to the victimized users. These fake sites can be used as vectors for other attacks. A report by Risk Based Security (2020) showed that, in the first three quarters of 2020, 21% of reported breaches involved ransomware, leading to compromised data. Health organizations and industries were unique targets given the public's reliance on health services. A report by Microsoft (2020) concluded that ransomware groups continued to target healthcare and critical services.[26] The Word Health Organization (WHO) in April of 2020 reported a fivefold increase in attacks and online fraud, which included a fictitious website where people donated to a solidary fund purportedly for COVID relief.

Compromised content. The desire for information during this pandemic is quite high. This means that people would tend to seek and share more information. An investigation by Verizon on data breaches in 2020 found that web application breaches accounted for 43% of all breaches and had doubled from those detected in the past year (Verizon, 2020a). Vulnerabilities were identified in certain default image and video viewers (Miyao, 2016; Bisson, 2019; Android Security Bulletin, 2019) in mobile phones and devices that could be exploited by bad actors.

Phishing and spoofing.[27] As an attack vector,[28] these two normally go hand-in-hand. A survey conducted by the private security firm Tessian in September 2020 found that 47% of respondents had clicked on a phishing email while working (Tessian, 2020). Google also reported that in one week in April of 2020 alone, 18 million daily phishing and malware emails related to COVID-19 had been detected (Lyons, 2020b). There has also been a reported increase in phishing attacks where bad actors send emails or messages pretending to be from relevant pandemic authorities like the WHO or a country's health ministry. Since a lot of people are working from home, the messages can also spoof their managers, banks, or business partners. These emails then ask users to click on links, perform tasks, or share information. This leads to further exploits, such as identity theft, transaction fraud, and many others.

Information leakage[29] and **credential dumps.**[30] Many of the exploits above can be used to cause information leakage. According to Risk Based Security (2020), there were 2,953 public breaches in the first three quarters of 2020, which points to a 51% decrease compared to the same period from the previous year. This can result in loss of intellectual property, use of information for blackmail (particularly health-related information), and data privacy[31] violations.

The Reenergized Need for Cybersecurity

> **Every technology-enabled advancement carries with it unique and new risks.**

It is no mystery why the public adoption of the Internet has taken off. The fundamental core of the Internet is the networking of information. The sharing of information leads to insights. Insights lead to ideas. Ideas lead to ideology and philosophy. Ideology and philosophy animate people to self-organize and take action. The time required for the diffusion of information and adoption of ideas has been faster than ever, following each change in the medium of dispersion. From books, to telegraphy, to radio and television, and now the Internet, the "action-reaction" cycle to information has been reduced from decades to hours.

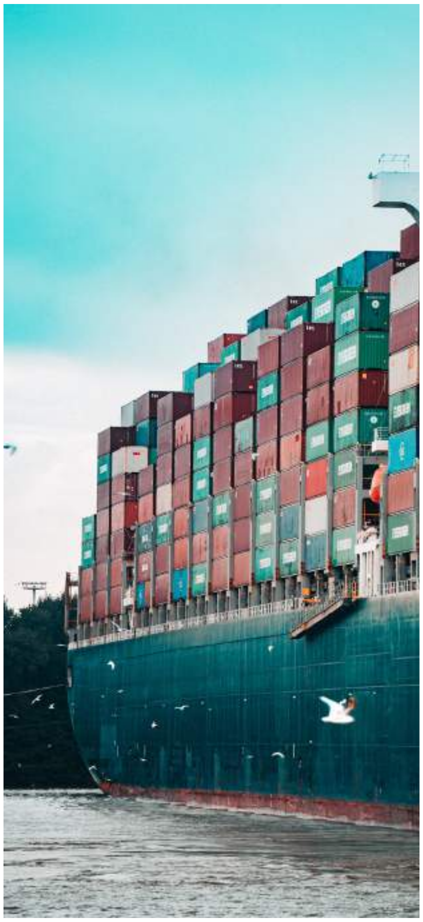
The narrative of the Internet, following its declassification as an asset of the U.S. defense establishment, was invariably "bright and sunny." There was close to a three-decade procession of scholarly articles projecting the benefits of globalization, unrestricted free trade, global social and economic upliftment, and the spread of liberal values. Discussions of misgivings or dysfunctional outcomes of the Internet were minimized as fringe concerns (Bergemann, 2002). The widening of income disparities, astronomical valuation of Internet companies, and the concentration of wealth in those who ran these Internet companies were accepted as inevitable but acceptable adjustments.

There is no doubting the numerous successes enabled by the Internet in distributing economic opportunities globally. These successes could be seen in the deepening integration of supply chains across countries as companies searched for the lowest cost and most reliable producer. For the Philippines, the business process outsourcing industry created a new source of service export earnings other than the remittances of overseas Filipino workers. This is the information economy version of traditional offshore manufacturing.

However, the pandemic and the tumultuous and acrimonious polarization of political discourses around the world were global systemic shocks. These shocks upended the comfortable assumptions and received wisdom regarding the Internet. If anything, these twin shocks exposed the fragility of social, economic, and political constructs. They reiterate, with even greater urgency, the need to prevent or at least mitigate the damage that could be wrought through greater consideration and implementation of cybersecurity measures.[32]

The pandemic exposed the limits of globalized supply chains and international cooperation. The world painfully realized the flawed logic of manufacturing only with the lowest cost producer at the expense of diversifying supply sources (Zhu et al., 2020). Countries that extensively manufactured personal protective equipment, for example, started canceling their confirmed exports and closed their trade borders instead, possibly in contravention of treaties (Shalal, 2020).

The credibility of the Internet as an information and news source was even further compromised. Its ability to provide timely and accurate analysis of information about the seriousness of the pandemic was put into question. Conflicting and incomplete pictures were presented by the media during the early stages of the pandemic. Social media was an early source of information as people sought to find a clearer assessment of what was happening on the ground in China, where the pandemic began. As skepticism and frustration grew about the reliability of traditional sources of news and information, social media filled the gap. Inaccurate and misleading social media posts, intentional or simply misguided, unfortunately followed. These all fed into the credibility gap between the citizenry, traditional media, and government.



The Internet also was the medium for launching scams and hacks that heightened public anxiety during the early months of the pandemic. Public healthcare systems were attacked, slowing down the response times of healthcare workers. Critical services of government and financial institutions in various corners of the world proved similarly vulnerable. In recent years, the promise of a network of interconnected physical objects linked to the Internet—the so-called Internet of Things—was seen as part of the next wave of digital evolution. That next step may be delayed, as trustworthiness of encryption and cybersecurity protocol used by such devices is paramount due to their potential to take down critical infrastructure.

The final noteworthy shock delivered by the pandemic is the overnight digitalization of social and business interaction as a result of sweeping lockdowns. Like nonswimmers suddenly thrown into the deep end of the pool, people quickly had to learn how to swim with digital interactions. Zoom meetings, food deliveries, and remote education again filled the gap. While economies retreated, they showed resilience and did not collapse. A year into the lockdown, societies have learned to conduct business and maintain family and social ties through their smartphones and laptops.

The emergence of enhanced or renewed threats associated with the technology shifts caused by the pandemic should not negate the benefits that result from digital transformation. Indeed, it is quite evident that every technology-enabled advancement carries with it unique and new risks. The Industrial Age resulted in unprecedented human-made pollution; the Atomic Age ushered in both atomic energy and the nuclear bomb. Often, the changes have been especially disruptive so as to overturn the long-accepted way of things. The fears arising from these changes and risks will always engender a generation of Luddites standing athwart the march of technology.

Endnotes

[1] “Data leakage” refers to any instance of access to data by unauthorized entities from within or outside an organization, whether accidental or intentional (Vodopyan, 2022). See also Breach.

[2] “Electronic commerce” or e-commerce encompasses the general concept of conducting commercial activities via the Internet (International Trade Administration, n.d.).

[3] “Work-from-home” or WFH is a term for a broad range of systems and methods for bringing traditionally office-bound work activities elsewhere, whether fully or partly. Also called remote work, telework, or home-based work (Aten, 2019).

[4] “Cloud services” here refers to the use of servers accessed through the Internet, as opposed to an organization’s own on-premises servers, to host the organization’s applications, data, and services. As the Internet allows for multiple points of connection, it is possible for a cloud server to provide services to more than one organization, or for an organization to obtain cloud services from a third-party provider. Cloud services can thereby help minimize business overhead related to maintaining a network, making them a popular option for organizations. For more information, see Chandrasekaran and Ananth (2016).

[5] A virtual private network or VPN involves the use of security protocols and technologies to allow access to an organization’s private servers through the public Internet, as if the user was on-site and directly connected to the network. For more information, see Chandra and Shenoy (2016).

[6] “Cryptography” refers to techniques intended to secure data and systems from unauthorized access, using codes, passwords, and authentication mechanisms, as well as provide security guarantees like confidentiality, integrity, availability, and nonrepudiation. For more information, see Springer (2017).

[7] “Virtualization” involves compartmentalizing systems or network resources on a single physical device, ensuring users are unable to access other users’ information. For more information, see Samarti and di Vimercati (2016).

[8] A business process outsourcing company, Everise, “moved 90 percent of their 12,000-strong support of customer service champions onto a secure Desktop as a Service (DaaS), work at home (W@H) solution in under two weeks during March 2020” (Cahiles-Magkilat, 2020).

[9] “Zero trust” refers to a network security approach that considers all users and devices untrusted by default, only providing access as-needed to properly verified users. For more information, see Kindervag (2016).

[10] “Antivirus”, also known as anti-malware, refers to software especially designed to monitor devices, systems, and networks for the presence of malware, addressing them automatically and alerting administrators as appropriate (Norton, n.d.). See also Malware.

[11] “Malware” is shorthand for malicious software, or any software designed to harm or exploit a device or network. For more information, see McAfee (n.d.).

[12] Ransomware victims that have backups are paying ransoms to stop hackers from leaking their stolen data (Palmer, 2021).

[13] Person-to-person and other “person-to” (P2X) transactions, such as person-to-business and person-to-government, have shown the largest shift. It is estimated that the share of digital P2X payments by volume is 9%–12%. P2X payments form about 80% of all transactions in the Philippines (Massally et al., 2019, p. 32).

[14] “Business email compromise” is a type of attack that involves manipulating employees into transferring money or information to criminals, using the hijacked or spoofed business email addresses of organization leadership. See Trend Micro (n.d.).

[15] “Phishing” and the related spoofing are a type of cyber scam that involves criminals pretending to be a trustworthy person or institution, in a bid to obtain personal and/or financial information from the victim. This

can involve asking a person via email or direct message or luring them into entering information into a fake website designed to look like a legitimate site, among other tactics. For more information, including guidance on how to avoid phishing, see U.S. Federal Trade Commission (n.d.).

16 “Cryptojacking” is a type of malware attack that takes over computer systems and uses them to mine for cryptocurrencies. For more information, see Nadeau (2021).

17 “Crimeware-as-a-service” refers to the criminal business model of selling cyberattack expertise to other criminals. For more information, see Avertium (2019).

18 “Dark web” is a general term used to describe Internet sites that are hidden behind specialized security protocols, designed to anonymize users and web hosts alike. These websites often act like private networks, requiring specific software or network configurations to gain access. For this reason, the dark web is often used for illicit activities by cybercriminals (Kaspersky, n.d.).

19 “Virtual private network provider” or VPN provider refers to any entity who hosts or operates a VPN for others (Cisco, n.d.). See Virtual Private Network.

20 “Breach” refers to any situation where an actor gains unauthorized access to a system, network, or device, often resulting in the loss or compromise of information (Office of Management and Budget, 2017). Also called data breach or security breach.

21 Over a decade later, Capital One was asked to pay a fine of $80 million after the data breach (Schroeder, 2020).

22 “Cloud security” encompasses the set of policies, controls, procedures, and technologies that protect cloud-based systems, data, and infrastructure. One of the key areas of cloud security is authorization or ensuring that only intended users have access to the cloud network or asset (Samarati & di Vimercati, 2016).

23 “EdTech” refers to a broad range of technologies, such as software or Internet platforms, designed for use in an education setting. For more information, see U.S. Department of Education (2017).

24 “Sensitive data,” as used in this publication, is any data access that can compromise the security of a person, organization, or any entity. In data privacy, and based on the Data Privacy Act of 2012, “sensitive personal data” is any information revealing an individual’s racial or ethnic origin, marital status, age and religious, philosophical, or political affiliations; their health, education, genetic [information], or sexual life; information issued specifically to an individual by the government, such as social security number; or any other information fundamental and traceable to that individual’s identity.

25 “Malicious actor” is a catch-all term for any entity, from nation-state-backed groups to rogue individuals, that aims to infiltrate or attack another entity’s ICT assets for their own ends (Johnson et al., 2016). Also called bad actor or threat actor.

26 “Critical services” refers to any service critical to widespread order, security, and functioning (European Banking Authority, 2015). See also Critical Infrastructure.

27 “Spoofing” refers to any type of cyberattack that involves tricking the victim into believing an email, a website, or other communications are from a trusted contact or organization, such as a bank (Fruhlinger, 2020b). Examples include websites designed to look like online banking pages or fraudulent emails that purport to be from a school or government body. Phishing is a specific kind of spoofing that lures victims into providing personal or sensitive information, such as birthdates and addresses, credit card details, or passwords (Belcic & Farrier, 2021).

28 “Attack vector” refers to “a method or pathway used by a hacker to access or penetrate” a computer or network (Sumologic, n.d.).

29 “Information leakage” refers to a software’s unintended release of sensitive data to unauthorized persons due to faults in the software. For more information, see NTT Application Security (n.d.). For an example of information leakage, see Lakshmanan (2020).

[30] "Credential dumping" refers to the extraction of usernames and passwords from a device's memory using specially created malware. For more details on dumping, see Greenberg (2019). For a case of credential dumping, see Palli (2020).

[31] "Data privacy" refers to the concept of securing personal information or any other sensitive data from unauthorized access and use. As a *legal right*, data privacy is a person's right to control any data about or originating from them (Cloudflare, n.d.-a).

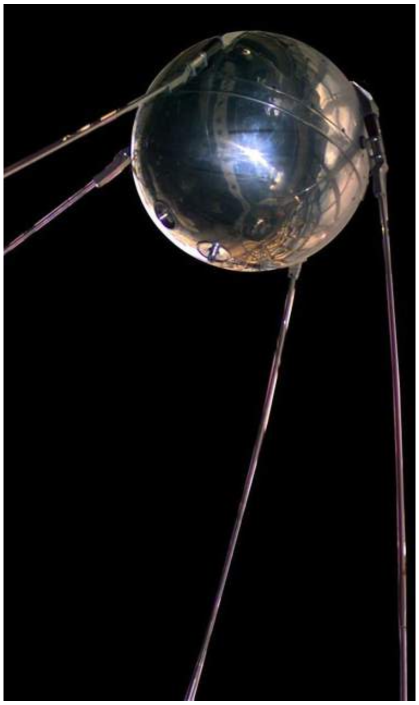
[32] "Cybersecurity measures" encompass the implementation of techniques, methods, or policies designed to improve an entity's cybersecurity posture (National Institute of Standards and Technology, 2015).

2 | The Internet-Enabled New World Order

> *The Internet has proven an efficient channel for the dissemination of information, thus enabling the rearrangement of the existing societal order.*

The Internet originated as an initiative of the U.S. government to advance its research capabilities as part of the country's defense posture. When the Internet itself shifted from a closed government network into a publicly shared space, the nature and targets of cyber threats would in turn evolve, with increasingly magnified impact.

A Brief History of the Internet



In 1957, at the height of the Cold War, the Soviet Union launched the first artificial satellite into orbit called *Prosteyshiy Sputnik-1* or *Sputnik*. The satellite's launch caught the U.S. government by surprise; it showed the Soviet Union's supremacy in science and technology. The perceived technology gap was unacceptable, and the responses of the U.S. government were deployed on multiple fronts. Among these responses was the establishment in 1958 of the Defense Advanced Research Projects Agency (DARPA) (Fuchs, 2010).

One of DARPA's projects was the Advanced Research Projects Agency Network (ARPANET), a network that would connect the various Pentagon-funded research institutions supported by DARPA. The practical aim was to have a communications network that would speed up information sharing among these research institutions (Lukasik, 2010). In the midst of the Cold War, the United States military had always wanted to develop a command-and-control network that did not have a single point of failure, capable of withstanding an enemy attack by using a distributed architecture. This thinking fed into the design of ARPANET as a decentralized network with no single control structure, foreshadowing how the Internet operates today.

Fundamentally, ARPANET was a network built for researchers to share their work in an open and collaborative environment. It was in the context of this research environment that Bob Kahn and Vint Cerf developed the transmission control protocol and Internet protocol[1] (TCP/IP), which is the core protocol that powers the Internet we know today. Supported by DARPA, it was also the addition of TCP/IP into the Unix-based Berkeley Standard Distribution (BSD) operating system that drove its adoption in these research and academic networks (Harris, 1998). The popularity and open nature of BSD Unix thus helped spread both TCP/IP and the Internet.

From the beginning, proposals concerning ARPANET's protocols and standards came from users (predominantly members of the scientific community) in the form of submitted Requests for Comment (RFCs). An RFC contained details on the proposed protocol but did not have to go through an approval process. RFCs remained unofficial in status, with researchers simply adopting the ones they found useful. The resulting standards selection thus embodied a process of adoption by merit involving the widest and broadest audience. This open meritocratic ecosystem is still the essence of how Internet standards are developed today under the Internet Engineering Task Force (IETF).

In the 1980s, ARPANET was essentially an open network; both authenticated and unauthenticated users could access the network and share files and documents. Anyone who had access to a system connected to an ARPA node could connect to the entire network (Leiner et al., 1997). However, not all users were connected to military research, especially as communities began to grow around the network. This created concern for the military establishment funding this network; thus, the civilian and military portions of the network were split, eventually leading to the birth of the Internet from a military research network.

This transition could not have been possible without Tim Berners-Lee, who in 1989 was working at the European Organization for Nuclear Research (CERN) (Noruzi, 2004). Looking for a way to easily publish information on the Internet for other users to access, Berners-Lee developed the World Wide Web (WWW). From a system for structuring and publishing research information, the WWW was quickly adopted by many different communities for other applications. A notable example is the development of the Internet search engine, as when David Filo and Jerry Yang started Yahoo! in 1994 (Aufa, 2018). Search engines made the Internet much more accessible to the average user. At around the same time, Jeff Bezos started Amazon to sell books online, demonstrating the Internet's utility in facilitating commerce and more (McFadden, 2021). From this point, the Internet started to reach a wider audience outside of academic and research communities.

Mirroring the global Internet's development, the Philippine Internet began when academic and research institutions wanted to establish a research network connected to the broader Internet. The first time the Philippines connected to the whole of the Internet was on March 29, 1994, when a connection was made between the University of San Carlos in Cebu and

Syracuse University in New York (Ayson, 2011). From these humble origins, an entire way of life in the Philippines was spawned because of the Internet. As of 2019, about 47% of Filipinos use the Internet, with 95% having access to social media (Albert et al., 2021). This number is expected to have increased significantly during the pandemic, as millions of Filipinos were forced to shift to online activities.

The Fragmentation of the Internet

> **Fragmentation is reflected in states becoming increasingly assertive with imposing their own rules, standards, etc., on content and technologies for their own national Internet networks.**

Over the past decade, there have been changes driven by “technological developments, government policies, and commercial practices” affecting the way the Internet operates (Drake et al., 2016, p. 7). Governmental fragmentation, which is caused by “government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information sources” (p. 4), is of particular concern as it could have the widest and most significant impact on citizens.

In their 2016 white paper for the World Economic Forum, Drake et al. described governmental fragmentation as the “global public Internet being divided into digitally bordered ‘national Internets.’” This can entail “establishing barriers that impede Internet technical functions, or block the flow of information and e-commerce over the infrastructure” (p. 5). In other words, states take jurisdiction or control over cyberspace through policy. Below are some examples of governmentally induced fragmentation of the Internet (p. 48):

1. Filtering and blocking websites, social networks, or other resources offering undesired contents
2. Attacks on information resources offering undesired contents
3. Digital protectionism blocking users’ access to and use of key platforms and tools for electronic commerce
4. Centralizing and terminating international interconnection
5. Attacks on national networks and key assets
6. Local data processing and/or retention requirements
7. Architectural or routing changes to keep data flows within a territory
8. Prohibitions on the transborder movement of certain categories of data
9. Strategies to construct “national Internet segments” or “cyber sovereignty”
10. International frameworks intended to legitimize restrictive practices

There are several examples pointing to how policy decisions of various nation-states have been changing the way people access the Internet or the content that can be accessed from it. The General Data Protection Regulation, for example, regulates the processing of personal data within the European Union. The Australian government passed a law in early 2021 requiring tech giants Google and Facebook to pay in order to link to or use news content. Some social networks are blocked in countries like Pakistan, Syria, Bangladesh, China, Iran, and North Korea. These policies and regulations are often driven by a country's own national interest and done in the name of national security.[2]

Some technological developments have also made the fragmentation more apparent (and global in scale) than others.

The emerging fifth generation (5G) of mobile wireless communication promises a quantum leap in connectivity. 5G moves the Internet out of the confines of applications residing in laptops and mobile devices, and into formerly "dumb" or unconnected devices (e.g., cars and household appliances) and machines formerly controlled by closed networks.[3] With 5G, these devices will be endowed with independence of action, without need of human intervention, and will coordinate and respond to each other's prompts or triggers. This vision for the future of the Internet is known as the Internet of Things (IoT).[4]

Artificial intelligence[5] and machine learning[6] are the base of IoT capability. Traffic signals adjusting their timing as more vehicles communicate their arrival; power generators boosting their output as air conditioners send out their temperature and blower settings; and delivery drones working in conjunction with mother-ship driverless trucks to inform hospitals when temperature-sensitive vaccines are to be expected—these are just a few potential IoT applications. Education systems will have to evolve as entire industries and occupations are transformed—in some cases diminished, if not totally eliminated—by IoT devices and artificial intelligence. Continuing education and retraining will be the norm for many workers to have a chance at maintaining gainful employment during their productive years.

All of the foregoing creates interesting possibilities for the future of societies and governance. The Internet has proven an efficient channel for the dissemination of information, thus enabling the rearrangement of the existing societal order. It has enabled disaggregation—as in the case of app-based ride-sharing services (also called transport network vehicle services) such as Uber—public transportation, and concentration, as in the case of the market dominance of Amazon. Similarly, it has enabled collaboration, as in outsourcing, and coercion, as in the case of the cancel culture.[7]

Fragmentation is reflected in states becoming increasingly assertive with imposing *their own rules*, standards, etc., on content and technologies *for their own national Internet networks*. And while the United States and China take center stage when it comes to Internet governance, different states have shown different ways of attempting to take control of the Internet and what and how their respective citizens can access and experience the Internet.

Because of the enormity of the Internet's potential, questions on the state's control of the online sphere are crucial. There are two fundamentally different schools of thought with respect to Internet governance: (1) today's Internet with an open and distributed standardization process and (2) an Internet under state control. These views also reflect the choice of technologies for the Internet.

What follows is a brief discussion of these two schools of thought, their geopolitical consequences, their implications on information security, and the need for responses in Philippine policy.

The Open Internet

> **The open Internet can be seen as an extension of the same democratic space that liberal states have endeavored to build offline.**

As Internet adoption increased around the world, its governance evolved as well. In the present Internet, the development of standards is based on open governance. The IETF and the World Wide Web Consortium (W3C) mainly governs standards development. The IETF relies on a Request for Comment[8] process that allows anybody to propose standards to be used on the Internet. This is an open standardization process—all RFCs are published online, freely available for anyone to adopt. This process is fundamentally opposite to a centralized top-down approach.

The principles underlying today's Internet are rooted in judicial philosophies formed through the United States' experience with regulating emerging digital technologies. Western concepts of privacy, personal security, and confidentiality have been translated and applied into electronic means of private communications. As social and commercial interactions migrated from physical to digital channels, laws evolved to ensure that these Western values and concepts are present in the digital world.

The emergence of new technologies, in conjunction with the legally recognized right to privacy of communications in the West, challenge the world's understanding of how these rights are practiced. The American Constitution's Fourth Amendment and related jurisprudence enshrine the concept of justifiable expectation of privacy[9] over traditional mail, protecting correspondence contained in a sealed envelope and sent through the postal system. Interference with the sealed envelope carries grave criminal liabilities for postal authorities, tantamount to a "warrantless search of private property" (Legal Information Institute, n.d.).

Yet, American jurists were slower to apply the same principle to electronic communications as the technology evolved from the telegraph to the telephone to the Internet. Wiretapping of phone calls despite the absence of an authorizing judicial warrant was upheld by the U.S. Supreme Court in 1928, notwithstanding the constitutional prohibition against unreasonable searches and seizures, in the landmark 1928 decision *Olmstead v. United States*, which would remain in force for 39 years. It was only in 1967, after the private nature of telephone conversations had become even more embedded into people's way of life, that the U.S. Supreme Court reversed course in *Katz v. United States*. The decision held that unauthorized wiretaps defied an individual's reasonable expectation of privacy and constituted violations of Fourth Amendment protections (Iannacci, 2018). The present-day widespread acceptance that communications are inherently private and insulated against undue state interference or interception informs not just jurisprudence but also legislation covering such matters as electronic commerce, cyber libel, digital privacy, and hacking.

The open Internet, informed as it is by virtues such as consensus building, freedom of information flow, and the promotion of individual rights, can thus be seen as an extension of the same democratic space that liberal states have endeavored to build offline. The dominant role of the United States in the development and emergence of the Internet helped assure that direction. However, an alternative model of the Internet informed by governments operating under different philosophical, social, political, and economic premises, has gained traction with the emerging strength of these states as well.

State-Controlled Internet

Central management is a key feature of this alternate model of the Internet. In countries such as China, which operates under tight state control, the Internet was introduced using a state-controlled and generally restricted model. This version of the Internet continues to recognize and exploit opportunities online to reach markets around the world in seconds. However, governments adopting this model also ensure that the Internet's potential to disrupt the state's well-crafted social order would be prevented through controls such as user traceability, censorship, and legal interception.

While the controls imposed by these states on the Internet primarily cater to imposing greater domestic regulations, it is possible that this alternate model would gain wider international acceptance and even be integrated in how the worldwide Internet operates.

In March 2020, China and a handful of equipment vendors proposed a new core Internet protocol (Gross & Murgia, 2020) at the International Telecommunication Union (ITU), the telecommunications and information and communications technology (ICT)[10] arm of the United Nations. The proposal argues that the current Internet protocols are insufficient to support future use cases, like IoT, machine-to-machine technology, and autonomous vehicles, necessitating a new protocol that can support these and other emerging technologies.

This was not the first time China attempted to make changes to what they perceive as a Western-oriented Internet. At the ITU Telecommunication Standardization Sector (ITU-T) World Conference on International Telecommunications 2012 (WCIT-12), one of the biggest items on the table was the review of the International Telecommunication Regulations (ITRs). These ITRs are considered the constitution of telecommunications and serve as the binding global treaty designed to facilitate international interconnection and interoperability of information and communication services. As part of the debates leading toward the revised ITRs, Russia, China, and other like-minded countries attempted to redefine the Internet as a system of government-controlled networks (Blue, 2012). This reflects these countries' view of how their own segments of the Internet are managed. There is a strong focus on information security, ability to censor information, and allowing state access to personal information. In the end, this process was quite divisive. Despite substantially toned-down wording, only 89 out of 144 countries represented signed the revised ITRs at the conference (ITU, 2012).

The proposals in WCIT-12, and now the "New IP" proposal in ITU-T, are examples of attempts to recreate the Internet with more state control. Previous draft proposals had made explicit statements, such as "Internet governance shall be effected through the development and application by governments," and "The sovereign right to establish and implement public policy, including international policy, on matters of Internet governance." In these assertions, the role of the state in Internet governance, including a top-down approach to defining standards, is front and center, as opposed to the more open system of governance of the current Internet (Blue, 2012). The proposals revolve around increased controls usually in the name of enhancing information security, a matter the state considers of utmost importance.

Some observers have remarked that the push toward greater state control is driven not only by China and like-minded regimes but also by certain European countries, which prefer the deterministic standardization process of the ITU-T (Gross, 2018). But within the Chinese tradition, there is a belief that sees individual rights as being circumscribed by an individual's role and context within society and the state. This belief has gained currency with governments and societies elsewhere over different periods of history, and it remains an open possibility that such an overarching philosophy will ultimately affect how the Internet operates.

While the most apparent approach is that of a bifurcation of the Internet, which reflects the competing Chinese and U.S. technology ecosystems, it is only one manifestation of the fragmentation of the global Internet. Actions of governments cannot be categorized simply as top-down or bottom-up. There is a wide spectrum of approaches that states take with regard to Internet governance. All national Internet networks employ a mix of these approaches, and how they differ depends on how willing governments are to impose top-down rules. Although different countries employ diverse approaches, *there seems to be a general trend* toward greater state control, even among liberal democracies such as Australia.

The Geopolitics of the Internet

Today's global Internet governance is characterized by a clash of these two paradigms: one envisions an open and more distributed Internet, while the other prefers a partitioned but centrally managed one. These divergent views create tensions among nations, particularly with regard to the establishment and rollout of new Internet infrastructure.

A growing number of states, such as the United States, the United Kingdom, India, and Canada, have banned Chinese telecom equipment companies from their communications network and from deploying 5G technology in their country.[11] Chinese-manufactured telecom equipment are compliant with the laws promulgated by the Chinese Communist Party (CCP).[12] Manufacturers are legally required to cooperate in state intelligence-gathering operations, potentially including those entities who sell their products and services overseas. This may effectively mean that the CCP has access to data passing through Chinese telecom equipment, not just in China but anywhere in the world (Robertson & Riley, 2018). Such access poses challenges to the data sovereignty of nations with telcos dependent on Chinese equipment.

Telcos with Chinese equipment embedded in their core infrastructure have claimed that the data encryption is more than sufficient to secure Internet traffic from any potential prying eyes (Valdez, 2019). Such explanations, however, may address the aspect of privacy but do not sufficiently pass the test of security. There is widespread acknowledgment that backdoors are common in home routers, network equipment, and software. The technical explanation is that "developers create [backdoors] to manage the gear" (Lepido, 2019). However, these backdoors can potentially be exploited by attackers or used for surveillance under the order of the governments.

Data security is not unique to the digital age. Data security is defined as the owner of the data having full control over access to the data as it travels from the sender to the receiver. In the case of physical mail or post, the post office is appointed by law to be the trusted courier of the envelope. At no point during the transit from sender to receiver will the post office delegate the responsibility of delivery of the envelope to a third party. In the case of Chinese telecom equipment, however, the data stream can be duplicated and harvested for information following decryption (Mühlberg, 2020).

Increasing state control over the Internet could affect fundamental rights, including the right to privacy, protection from unreasonable search and seizure, and free speech. These competing values lie at the heart of the bifurcation of the Internet and do not concede to easy solutions, considering the extent that these bifurcated segments of the Internet still interact with each other.

The track record of Internet standardization can be seen in terms of standards organizations. The ITU-T, which is more centralized with states, creates stable standards but is slow and deliberate. The open IETF process, on the other hand, allows for the rapid creation of standards, with such speed more responsive to market needs. The high adoption of consensus-built IETF standards today indicates the process's popularity vis-à-vis the more centralized approach of the ITU-T.

The prevailing philosophy in Internet governance influences cybersecurity policy as well. Centralized state governance necessarily implies a centralized approach to identifying and resolving information security issues. A centralized solution forces a one-size-fits-all mindset and may not be responsive enough to support market needs. It locks the technology to a particular point in time, making it easier to date.

A Brief History of Cybersecurity

> **Despite, or perhaps because of, the widespread growth and use of the Internet, there persist many issues that compromise the security of those who participate in any online activity.**

Given the Internet's origins as a relatively open research network designed to share information, a closed-door security policy was not exactly built into its design. The key protocols that power the Internet, such as hypertext transfer protocol (HTTP) and TCP/IP, were originally designed to maximize research and information sharing; anybody with access to the system could use the system. Host-based controls were yet to be strengthened and any user could essentially replace applications and services with versions of their own. In fact, the inherent lack of security and the emerging need to isolate military from civilian use cases ultimately led to the privatization of the Internet (Frischmann, 2001).

Despite, or perhaps because of, the widespread growth and use of the Internet, there persist many issues that compromise the security of those who participate in any online activity. Some of these issues are discussed in this section.

Domain Name System

The Domain Name System (DNS) is a system for identifying computers, services, or other resources connected to the Internet, each of which are assigned domain names (Cloudflare, n.d.-b). Prior to the adoption of DNS, or in the early days of ARPANET, the list of hosts and their addresses were stored in a single file called HOSTS.TXT, which was managed by the Network Information Center at the Stanford Research Institute (Mockapetris & Dunlap, 1988). This file was then distributed to each of the nodes in the ARPANET—a workable system when there were just a few hosts on the network. However, this ultimately led to concerns involving scalability, timeliness, and—most crucially—security. As the files reside on each node, each node owner can effectively edit the file to reroute traffic. This allowed the node owner to change the entry with the permission of the Network Information Center or the owner of that node entry.

DNS was ultimately adopted in order to mitigate these security issues; however, they have not been fully extinguished. In 2008, Dan Kaminsky revealed a potential vulnerability[13] due to the nature of DNS that enabled an exploit called DNS poisoning. This allows attackers to trick users into visiting arbitrary hosts defined by them in lieu of their intended destinations, effectively redirecting traffic. In the same year, telecom company AT&T had a major attack on their DNS servers (*The Toronto Star*, 2008). This attack redirected users of AT&T DNS services (including retail and corporate customers) to arbitrary sites. The problem was not easy to fix because this type of security issue was not factored into the design of the DNS protocol.

Eventually, issues like these led to the development and adoption of an even more secure protocol called Domain Name System Security Extensions (DNSSEC) (Southam, 2014). To date, DNSSEC has yet to be widely adopted. There remain cases of DNS poisoning attacks, a notable example being that which affected Amazon Web Services in 2018 (Nation, 2018). DNS poisoning attacks demonstrate that security was not integrated into the Internet's design from the beginning.

Internet Worms

On November 2, 1988, Robert Tappan Morris wrote a self-replicating application on the computers of the Massachusetts Institute of Technology, which would come to be known as the first-ever Internet worm (Spafford, 1989). This application began spreading across the network to other research institutions, infecting 1 out of 10 hosts on the Internet within 24 hours. Unlike computer viruses, worms have the ability to self-propagate secretly across a network (Latto, 2021).

The Morris worm was not designed to delete files or remove users; it simply spread itself as widely and secretly as possible. This was easy on the early Internet, a trusting community where everybody kept their doors open. After the Morris worm and its ensuing damage, that atmosphere of trust was diminished. The Morris worm opened the eyes of many systems and network operators on the importance of information security.[14] Today, doors on systems and networks are locked by default.

Internet Viruses

In 2000, a new piece of malware, originating from the Philippines, spread across the Internet. Known as the ILOVEYOU virus, it is considered the first truly global computer virus, believed to have infected tens of millions of computers, inflicting damage estimated at USD 10 billion. The virus operated by sending itself in an email with the subject "ILOVEYOU." The email contained a VBScript disguised as a file attachment that when clicked would replicate itself by automatically sending itself to more victims listed in the user's contact book. These emails would then appear as if they were sent by the victim (Wolber, 2016).

This form of exploitation eventually became known as phishing. What made the ILOVEYOU virus so effective was that it exploited a very human vulnerability: the need to receive affection. This points to a very real concern when looking into information security aspects of a global network like the Internet. Disconcertingly, an interconnected global network such as the Internet is only as strong as its weakest user—a concern that should inform information security analytics. Defense strategies against viruses, even if deployed by organizations, should thus focus on developing the capacity of individuals to employ security practices as part of their daily online routine. To that end, organizations should not hesitate in investing in information security awareness programs targeting their members.

It would likewise be foolhardy to deem worms and viruses as mere tools of vandalism or products of curiosity gone awry. As with the Morris worm and the ILOVEYOU virus, they demonstrate the vulnerabilities of systems and their users that can be exploited to greater effect by bad actors. Anytime the effectiveness of such malware is so publicly demonstrated, there is greater incentive for bad actors to capitalize on such tools. Worryingly, there have been instances where such online vulnerabilities have been systematically weaponized.

Stuxnet and Weaponizing the Internet

In 2010, centrifuges used to enrich uranium gas in the Natanz uranium enrichment plant in Iran were failing at an unusual rate. It was later discovered that the control systems of these centrifuges were infected by a piece of malware now more commonly known as Stuxnet (Zetter, 2014).

Stuxnet is an example of a purposely designed malware, in this case targeted at disrupting Iran's nuclear program. It was reportedly developed by a nation-state, specifically engineered to bridge air gaps to get to its target in a stealthy manner. Stuxnet was able to replicate in computers running Windows, even those not connected over the Internet, allowing the worm to spread over local area networks (Kushner, 2013).

Stuxnet would have remained covert if the malware did not inadvertently spread beyond its specific targets, toward the Internet at large (Kerr et al., 2010, p. 2). There are indications that other malware developers have since copied Stuxnet, repurposing it to focus on gathering information rather than on interfering with industrial operations (Bencsáth et al., 2012).

The ability to weaponize the Internet using malware like Stuxnet is certainly not limited to nation-states. It can be deployed by a wide range of bad actors from organized crime groups, to corporations, to a bored student in a garage. The multiple sources of danger mandate increased consciousness and responses to cybersecurity threats.

Given these evolving cybersecurity challenges, how have nation-states and regional organizations armed themselves to fight against the various risks and threats found on the Internet?

Endnotes

1 “Internet protocol,” or IP, refers to the set of rules for routing and addressing packets of data so they can travel across the multiple networks making up the public Internet. IP ensures that data packets arrive at the right destination. To identify devices connected to the Internet for routing purposes, all these devices are given an identifier called an IP address (Cloudflare, n.d.-c).

2 “National security” refers to the protection and defense of a country’s citizens and their well-being, both physically and economically. Issues affecting national security can be national *in scope* if they directly affect a large number of persons in the country, or *in impact*, if the consequences thereof have implications for a significant proportion of the country (Osisanya, n.d.).

3 In addition to the substantive increase in data requirements and rates, an ongoing challenge for 5G mobile Internet networks deals with how to link billions of smart devices, including not only traditional smartphones but also smart consumer products, wearables/implantables, sensors in mobile IoT extensions, and more. For more information, see Morais and Obar (2018).

4 The IoT paradigm describes communication not only human to human but also machine to machine without the need of human interference. For more information, see Goudos et al. (2017).

5 “Artificial intelligence” encompasses intelligent machines or computer programs that process information with minimal human input and are therefore capable of independent analysis, forecasting, and problem-solving. Also used to describe the field of study and technological development involving the creation of machines that can learn from experience and adjust to new inputs with human-like acuity (IBM Cloud Learn Hub, 2020). See also Machine Learning.

6 “Machine learning” is a software paradigm involving the use of large data sets to “train” or improve the software’s processing and interpretation of data (IBM, n.d.-a).

7 “Cancel culture” is the phenomenon wherein groups of people, often in social media platforms, culturally block a person from having a prominent public platform or career. Through boycotts or public calls for employer sanctions, individuals use this avenue for social justice to bring powerful people to account.

8 “Request for comment,” or RFC, is a stakeholder-driven development process, commonly associated with the Internet Engineering Task Force’s standards development, that allows anybody to propose technical specifications or standards to be used on the Internet. All RFCs are published online and are adopted on a voluntary basis (Borchert et al., 2021).

9 The concept of justifiable expectation of privacy originates from *Katz v. United States* and is established using a two-part test. For more, see Legal Information Institute (n.d.).

10 “Information and communications technology,” or ICT, is a family of related electronic, primarily digital technologies, that enable access to vast amounts of stored information, or the transfer of data between users. A common thread among ICTs is that they allow users to interact with data—send, receive, process, and store it, to name a few activities (Food and Agriculture Organization AIMS, n.d.).

11 The move to ban Chinese telecom equipment in some countries may have started after the director of the U.S. Federal Bureau of Investigation warned in early 2018 against buying Huawei and ZTE phones. See Keane (2021) for the timeline.

12 Lawful interception in telecommunications is not limited to China. Some countries allow lawful interception under certain conditions. See, for example, the European Union’s (1995) Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications. In fact, telecommunications systems have always had this capability. However, the early Internet’s users, composed primarily of academics and enthusiasts, were averse to censorship or infringements on privacy—perhaps more so than today. As Internet standards spread via voluntary adoption, lawful interception was thus not among the features baked into the Internet’s architecture.

13 “Vulnerability,” in cybersecurity, is any flaw or oversight in a device’s, system’s, or network’s design,

whether physical, technological, or even social, that can be exploited by attackers to do harm (National Institute of Standards and Technology, 2006).

14 “Information security” refers to the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Scholl et al., 2008).

3 | Regional and National Cybersecurity Frameworks

> *A comprehensive, robust national framework aligned with global best practices is an essential tool in the task of securing cyberspace.*

When it comes to the security of information and communications systems and networks as well as the data stored in databases, quick and decisive action is necessary to forestall or mitigate harm from cyberattacks or breaches. A cybersecurity strategic plan that is regularly updated to keep up with the latest technological developments and lessons learned from cyberattacks and malicious activities would provide a guide in building an organization's or a country's strong and resilient cybersecurity posture.

Cybersecurity has the distinct characteristic of not recognizing borders or boundaries. While policies are specific to countries, threats—and threat actors—take advantage of any vulnerable target, wherever they may be. Cybersecurity, therefore, increasingly relies on cross-border cooperation, allowing threats to be addressed even if they reside outside the target's jurisdiction.

The North Atlantic Treaty Organization (NATO) recognizes three dimensions of cybersecurity activity: government, national, and international (Klimburg, 2012). Of these, the international dimension most closely maps to the Internet's globalized nature, whose biggest players (such as content providers, like YouTube, or social media sites, like Facebook)—and users—are not bound to a single country's policies. International and regional frameworks recognize that "for any nation state or interest group, to advance its interests requires collaboration with a wide range of international partners" (Klimburg, 2012, p. 10).

International and Regional Frameworks[1]

One of the earliest and most prominent of the international frameworks on cybersecurity was the Budapest Convention on Cybercrime (also called The Budapest Convention), first ratified on November 23, 2001. It is a treaty obligation ratified by 68 states, including the Philippines (Council of Europe, 2021).

The Budapest Convention aims to broadly harmonize the treatment of cybercrime and allow for a level of equivalence between the policies of signatory countries—i.e., "a common criminal policy" to protect against cybercrime by laying out policy directions for local national policies, as well as mechanisms for international cooperation (Council of Europe, n.d.). The Budapest Convention also addresses issues involving the international pursuit of cybersecurity, particularly jurisdiction in the prosecution of cybercrime, extradition agreements, and other general areas of cooperation.

To date, the Budapest Convention remains the only international/regional framework pertaining to cybersecurity with the status of a treaty obligation. However, other intergovernmental organizations have implemented working arrangements meant to facilitate cross-border cooperation on cybersecurity.

In the European Union, the EU Cybersecurity Act of 2019 mandates the EU Agency for Cybersecurity (ENISA) to create a European cybersecurity certification framework that would see products and services undergo a single certification process throughout the Union. ENISA is also responsible for developing and promulgating technical standards, and developing advice for their implementation in both public and private sector organizations (Eurosmart, 2019).

In Asia, the Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group has a Security and Prosperity Steering Group focused on cybersecurity. In November 2019, four years after it was first proposed, the APEC Framework for Securing the Digital Economy was released, providing nonbinding principles and strategic recommendations to inform member economies as they develop their own policy and regulatory frameworks (Telecommunications and Information Working Group, 2019).

During the drafting process, APEC member countries expressed reservations about outlining specific approaches to cybersecurity in the framework. Instead, the framework identifies seven general strategies that will help facilitate cross-border trade, investment, and economic growth: digital security risk management, resilient critical information infrastructure, digital user empowerment, personal data security, develop economic strategies, strengthen collaboration, and digital security technologies for trust (Telecommunications and Information Working Group, 2019, p. 9).

As a nonbinding, recommendatory document, the APEC framework most closely resembles the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is similarly voluntary.

The NIST framework is centered around a set of core functions that will help an organization achieve a robust cybersecurity posture. These functions are as follows (NIST, 2018b, p. 14):

- *Identify* — Identifying risks and threats to systems, people, assets, data, and technology
- *Protect* — Implementing the appropriate safeguards to ensure critical systems and information are secure
- *Detect* — Ensuring that threats are identified in a timely manner, if and when they happen
- *Respond* — Having well-thought-out responses to detected threats, containing the harm of an attack
- *Recover* — Creating mechanisms to ensure the continued functioning of the organization after an attack, including restoring any lost service or data

Unlike the Budapest Convention and the APEC framework, which are meant to guide the national policies of participating countries, the NIST framework is designed to be adopted by any organization, whether public or private, of any size, and wherever situated in the world. It also espouses more general principles that are applicable regardless of legal context. Hence, the NIST framework can serve as an international framework, despite being developed by the U.S. government.

There also exist international frameworks for more specific areas or applications. For example, the Cooperative Cyber Defence Centre of Excellence of NATO publishes the *Tallin Manual on the International Law Applicable to Cyber Warfare*, meant to guide member and other countries on the legal conduct of state/military cyber operations online (Schmitt, 2013). These frameworks allow users to cater to the specific cybersecurity concerns they may have depending on their field.

The Clean Network Initiative is another notable multilateral effort launched by the United States in 2020, which is overtly premised on the lack of trust in Chinese digital technology (U.S. Department of State, 2021). The Clean Network Initiative seeks to promote internationally accepted and technologically neutral standards of digital trust developed by the Center for Strategic and International Studies, the European Union’s 5G Toolbox, and the Prague Proposals on the importance of security of 5G networks. Over 30 leading mobile operators from 20 countries have signed on to the Clean Network Initiative, with the net effect of excluding components produced by Chinese government affiliates in 5G networks (Layton, 2020).

Elements Behind National Strategies and Frameworks

Notwithstanding multilateral frameworks, it has proven to be in the interest of individual countries to address their own cybersecurity concerns, particularly the need to protect systems, networks, devices, and data, whether they are stored in databases or are in transit. A comprehensive, robust national framework aligned with global best practices is an essential tool in the task of securing cyberspace. Questions as fundamental as what constitutes cybersecurity, who is to be responsible for it, and what protections will be put in place will be determined by a cybersecurity framework.

> **Globally, the general norm among cybersecurity policies is the peaceful use of cyberspace.**

Although cyberspace transcends borders, a national cybersecurity framework is necessary to guide the behavior of human actors, all of whom are bound by their local laws. This must be complemented by a regional mechanism for cooperation, particularly regarding prosecuting cybercrime. All of these are areas that the Philippine government should look into, and individual organizations must consider, to ensure that the country is no less secure than its peers in the region and around the world.

The following is a brief overview of the elements common among national frameworks, along with case examples from selected countries. These represent a shared focus on areas that different governments agree deserve to be prioritized.

Economic Growth and Prosperity

Some countries espouse economic growth and prosperity as one of the aims of their cybersecurity strategies. In a more direct and limited sense, this can refer to the development of a local cybersecurity industry, as stated by Brunei (Marco et al., 2018), Malaysia (National Cyber Security Agency [NACSA], 2020), and Singapore (Cyber Security Agency, 2016) as part of their respective national frameworks. Research and development in the field of cybersecurity is vital, and support is necessary from governments to incentivize research and development, as well as innovation.

Defined Cybersecurity Policies

Policies set certain norms that may be enshrined in laws and regulations. Some countries have, therefore, promulgated laws that specifically address cybersecurity and cybercrime. Formal cybersecurity policies recognize the importance of government and business organizations putting in place cybersecurity governance frameworks that establish acceptable norms of behavior in cyberspace.

Globally, the general norm among cybersecurity policies is the peaceful use of cyberspace. These policies help uphold the ideal of a free, open, and secure Internet that seeks to balance privacy, freedom, and human rights. One of the four core values of New Zealand's Cybersecurity Plan, for example, is that "people are secure and human rights are respected online" (Department of the Prime Minister and Cabinet New Zealand, 2019, p. 9). Similarly, Canada's National Cyber Security Strategy commits the country's government to a cybersecurity approach that "promotes and protects rights and freedom online" (Public Safety Canada, 2018, p. 3).

The creation and designation of an agency of government that will address cybersecurity matters is another important issue that must be covered by policy. Both Brunei and Singapore identify (and in the former's case, create) national cybersecurity agencies tasked with overseeing, coordinating, and responding to any cybersecurity-related issues and threats.

In the same vein, defined cybersecurity policies may also cover the development of a national cybersecurity system, as is the case for Cambodia (Telecommunication Regulator of Cambodia, 2014) and, to a lesser extent, Malaysia (NACSA, 2020). Consistent with putting in place a cybersecurity governance framework, policies should also cover the adoption of cybersecurity standards and metrics. Vietnam's Law on Network Information Security goes so far as to provide regulations on technical standards and norms of network security, for both the government and the private sector (United Nations Institute for Department Research, 2021).

A formalized risk management approach to cybersecurity seeks to identify and assess risks associated with threats to information systems and vulnerabilities of information systems. As a matter of policy, cybersecurity risk management may be adopted not just by private organizations but also by nations themselves, to identify and properly address risks. Malaysia is developing a standard cybersecurity risk assessment framework for use by all stakeholders, but particularly for sectors considered critical national information infrastructure (NACSA, 2020). Australia, on the other hand, uses a risk assessment framework for systems in use by government bodies (Department of Home Affairs [DHA], 2016, pp. 10–11).

In terms of technology, protocols that enable and guide device and network interactions continue to evolve. New and emergent technologies such as artificial intelligence, quantum computing, cloud computing, and others present new challenges in cybersecurity. All these have resulted from the autonomous development of the Internet, with various entities independently addressing a piece of the puzzle that makes up cyberspace. Japan's Cybersecurity Strategy 2018 emphasizes the importance of maintaining autonomy on the Internet, both from a rights-based perspective and to ensure security through a diversity of systems. Both the Philippines (Department of Information and Communications Technology [DICT], 2017) and South Korea (National Security Office, 2019) also espouse autonomy as a key principle of their cybersecurity frameworks.

Cybersecurity Culture

The development of a cybersecurity culture is an essential challenge that countries must address. Without it, individuals, businesses, governments, and the general public will continue to be exposed and may fall victim to cyber threats and attacks.

The development of a cybersecurity culture can start at delivering cybersecurity awareness programs. In organizations, public and private, leadership and employee buy-in is important. It is even more challenging to create cybersecurity awareness addressed to the general public—a challenge that the government may address by developing education programs to be delivered in schools.

Of particular importance is developing a security culture among professionals and other members of the workforce. In many cases this translates to a desire for a highly skilled cybersecurity workforce. As such, Australia considers it a priority to "develop a highly skilled cybersecurity workforce, starting with academic centers of cybersecurity excellence" (DHA, 2016, p. 11), while the United States lists the development of a "superior cybersecurity workforce" among its National Cyber Strategy's key goals (The White House, 2018, p. 17). Countries as diverse as Cambodia, China, New Zealand, and South Korea all emphasize the development of a cybersecurity culture in their national frameworks (Christine & Thinyane, 2020).

Researchers and developers can also benefit from other global experts through established international cooperation and information-sharing mechanisms. Partnerships between and among government, businesses, and the academe/research institutions should be encouraged.

Computer Emergency Response Teams

A computer emergency response team (CERT) refers to a group of experts who respond to cybersecurity incidents. However, the role of CERTs has evolved over the years to include cybersecurity incident monitoring and reporting, malware analysis, cybersecurity awareness and training, among others. Some countries also indicate cyber threat/cyberattack response, protect/secure cyberspace, and strong cybersecurity/defenses/defend systems among the areas handled by CERTs.

CERTs can serve as an important pillar of a national cybersecurity framework. Cambodia, for instance, counts the enhancement of its CERT system as one of the most important targets for its cybersecurity strategy (Telecommunication Regulator of Cambodia, 2014). Similarly, national CERTs are a keystone of Malaysia's cybersecurity emergency readiness thrust, as stated in their National Cyber Security Policy (NACSA, 2020).

While countries may organize their own national-level CERTs, CERTs can also be found in business and industry. A CERT may also be just a section in an organization's information security operations center. In any case, international cooperation is one significant activity of CERTs that has led to the development of CERT practices. CERTs also have organized themselves into international or regional groups to exchange and share information on information security incidents.

For this reason, CERTs can act as the frontline of international cooperation for day-to-day cybersecurity practice. Brunei, for example, recognizes that the Brunei CERT (BruCERT) laid the foundation for its international linkages, facilitating information sharing and the exchange of best practices (Marco et al., 2018). CERTs allow governments, business organizations, the academe, and citizens to cooperate and collaborate in addressing cybersecurity/information security issues in order to develop response mechanisms.

Cybercrime

The cybercrime landscape continues to evolve as Internet technology evolves. Cybercrime is particularly challenging, considering its transnational and borderless character and the ephemeral and fleeting nature of digital evidence. Law enforcement agencies are, therefore, faced with the challenge of understanding the different country context of cybercrime laws, particularly when issues of jurisdiction and prosecution are involved. Brunei, Malaysia, and Thailand, for example, focus on the need to develop cyber-capable law enforcers and adopt law enforcement standards in their cybersecurity strategies. Other countries, meanwhile, such as Canada, China, and Singapore, seek to address the proliferation of cybercrime safe havens.

National Security

Critical infrastructure protection is a matter of national security concern (NIST, n.d.). Critical infrastructure operations have increasingly been dependent on information systems. An attack on a critical infrastructure can have a devastating effect on a nation's physical or economic security, peace and order, or the health and safety of citizens and residents.

> **An attack on a critical infrastructure can have a devastating effect on a nation's physical or economic security, peace and order, or the health and safety of citizens and residents.**

A review of 17 countries' national cybersecurity frameworks revealed 10 had stated strategies on the protection of critical infrastructure. The Philippines' National Cybersecurity Plan, for example, lists the protection of critical information infrastructure first among a list of objectives. Similarly, Malaysia's National Cybersecurity Policy puts addressing risks to critical national information infrastructure at the top of their priorities. China, on the other hand, equates the protection of critical infrastructure to the defense of sovereignty and of national security itself.

Cyberattacks and cybercrime affect both the public and private sectors. The extent to which cybersecurity is regarded as a national security matter and the issue of sovereignty in or of cyberspace depend on a country's national security policy.

Table 1 compares the common threads in the national cybersecurity frameworks and policies of select countries.

Table 1. Common Threads in National Security Frameworks of Select Countries

Elements of a national cybersecurity strategy	**Australia**	**China**	**Indonesia**	**Philippines**	**US**
Stakeholders:					
Academe / research community	●				
Business	●			●	●
Citizens	●			●	●
Critical infrastructure			●	●	●
Government	●			●	●
Focus Areas:					
Advocacy: free, open, and secure Internet	●	●			
Autonomous development of cyberspace					
CERT / CSIRT*				●	
Critical infrastructure protection		●	●	●	●
Cyber-capable law enforcers / law enforcement standards					
Cybersecurity awareness / education	●			●	
Cybersecurity culture					
Cybersecurity skills and knowledge developed; cybersecurity workforce	●			●	●
Cybersecurity standard and metrics					
Cyber threat / cyberattack response		●		●	
Cyber threat / information sharing	●	●			
Economic growth and prosperity	●				●
Growth of cybersecurity business / industry	●				
Incident monitoring and reporting					●

**CERT: computer emergency response team; CSIRT: computer security incident response team*

Table 1. Continued

Elements of a national cybersecurity strategy	**Australia**	**China**	**Indonesia**	**Philippines**	**US**
International and regional cooperation / in-country cooperation / collaboration	●	●		●	
National cybersecurity system					
National security		●	●		
National sovereignty / sovereignty of cyberspace		●			
Network and cybersecurity governance	●	●			
Organizational reform - creation of an agency which will coordinate all matters on cybersecurity					
Partnerships: Government, business, academe / research community	●				
Peaceful use of cyberspace		●			
Policy, legislation, and rule of law		●		●	
Privacy, freedom, and human rights protection				●	
Protect / secure cyberspace		●			
Protection from cybercrime / shutdown safe havens	●	●			●
R&D, innovation	●	●	●		
Risk management				●	
Strengthen government in terms of cybersecurity					
Strong cybersecurity / defenses / defend systems	●	●		●	●

Cybersecurity Governance Frameworks of Select Nations

In alignment with the global nature of cybersecurity concerns, it is inevitable that nations seeking to enhance their own national frameworks will look to the best practices or proven practices of other nations. However, the blind adoption of foreign models without understanding the national contexts that inform these other frameworks would ultimately be foolhardy.

The succeeding discussion dwells on the cybersecurity governance frameworks of five nations: Australia, China, Israel, Russia, and the United States. Each has unique offline systems of government, geopolitical interests, and domestic concerns that bear particular influence in the development of their own cybersecurity policies.

Australia

Australia is the 6th most cyberattacked country in the world, with 16 cyberattacks, from state actors and cybercriminals, from May 2006 to June 2020 (Specops, 2020). Aside from government networks, the attacks are particularly hitting small businesses, which make up 94% of Australian businesses (Business Australia, 2020). The Department of Home Affairs estimates that cybersecurity incidents cost Australian businesses up to USD 29 billion each year (*The Daily Telegraph*, 2019).

As early as 2000, cyberattacks have been identified by Australia's Department of Defence (DOD) as an emerging security challenge (DOD Australia, 2000). Prime Minister Kevin Rudd in 2008 acknowledged to the Parliament that cyber threat is one of the top-tier national security priorities of the government (Rudd, 2008). On June 19, 2020, Australian Prime Minister Scott Morrison made a formal announcement that Australian organizations are the target of sustained cyber activities by a sophisticated state actor (Prime Minister's Office, 2020). The prevalence and increasing sophistication of the cyber threats have prompted the Australian government to adopt robust unilateral and multilateral measures in the field of cybersecurity.

The Australian government is active in building international cooperation in cyberspace, noting the borderless nature of the Internet and cyber threats. In 2016, it created the position of ambassador of cyber affairs within the Department of Foreign Affairs and Trade (DFAT). The cyber affairs ambassador leads the government's international cybersecurity policy interests and works with other nations to champion an Internet that is open and secure.

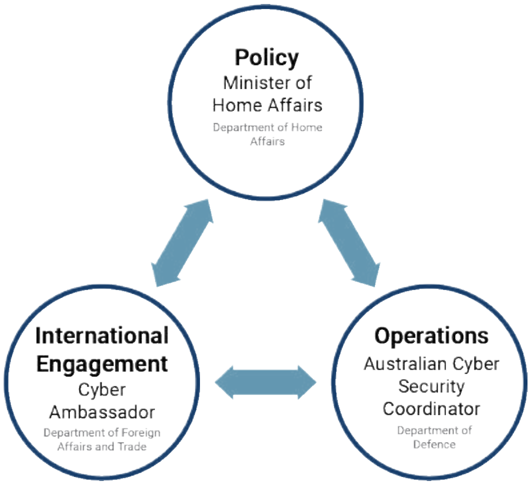
Governance Structure

The Australian government has adopted a multiagency approach to cyber governance. Over the years, there have been significant changes in the agency with the lead role in cyber policy because of government reshuffling.

Cybersecurity policy development had initially been the responsibility of the Attorney General's Department. During the time of Prime Minister Gillard (2010–2013), cyber policy was transferred to Australia's Department of the Prime Minister and Cabinet (2012). In 2017, the lead agency for cyber policy was again transferred to the DHA.

During his tenure, Prime Minister Malcolm Turnbull (2015–2018) had appointed a dedicated cybersecurity minister as part of his cabinet, yet the position was abolished during the subsequent premiership of Scott Morrison. The private sector called on the Australian government to return the position to the cabinet, arguing that someone must have the dedicated authority in, and responsibility of, cybersecurity (Stilgherrian, 2019b).

Figure 1. Australian Government's Cybersecurity Arrangements


Policy
Minister of Home Affairs
Department of Home Affairs
International Engagement
Cyber Ambassador
Department of Foreign Affairs and Trade
Operations
Australian Cyber Security Coordinator
Department of Defence

Note. Adapted from *Australia's Cyber Security Strategy,* by Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2016 (https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf). CC BY 4.0.

The DHA is responsible for all policy affairs involving safety and security within Australian borders, including cybersecurity. The department, established in 2017, was the product of wider reforms within the Australian government that restructured security policymaking to have a more civilian character. Today, the DHA leads the development of the country's cybersecurity policy, including the implementation of Australia's national cybersecurity strategy.

Within the DHA, the national cybersecurity adviser provides input on any policies and projects promulgated by the department, and the Cyber Security Policy Division develops the country's cybersecurity strategy, a responsibility previously assigned to various wings of the government.

As a federation, Australia's states and territories are also free to promulgate cybersecurity policies that complement the national strategy. The state of South Australia, for example, developed its own South Australian Cyber Security Strategic Plan 2018–2021. Similarly, other departments and offices of the national government are also encouraged to formulate cybersecurity strategies specific to their organization's needs and characteristics, as with Services Australia's Cyber Security Strategy 2018–2022.

The DHA's national cyber coordinator ensures that the plans set by government offices at various levels, along with those of the private sector, civil society, and the academe, are designed and implemented in harmony with the national strategy's tenor. The coordinator is also the department's main point of contact with DFAT (for the Office of the Ambassador for Cyber Affairs) and the Department of Defense (for the Australian Cyber Security Centre or ACSC.)

Alongside the DHA, the ACSC within the Australian Signals Directorate (ASD) under the Department of Defense works to improve the country's general cybersecurity posture. The ACSC monitors cybersecurity threats, provides advice to mitigate threats, and responds to cyber incidents. It works closely with private and public organizations and operates a 24-hour cyber hotline to provide a timely response to attacks. It also prepares the country's annual cyber threat report, which identifies and describes key cybersecurity threats targeting Australian systems and networks (ACSC, 2021b). To fulfill these responsibilities, the ACSC houses CERT Australia, the national computer emergency response team (ASD, n.d.).

Although officially part of the Department of Defense, the ACSC strives to operate an open, stakeholder-driven process for advancing the country's cybersecurity capabilities. It operates a network of Joint Cyber Security Centres responsible for coordinating research and information-sharing across the government, private sector, civil society, and the academe (ACSC, 2021a).

Historically, the bulk of Australia's cybersecurity tasks fell to the ACSC to see through. With the establishment of the DHA, however, implementation of the national strategy is now firmly a responsibility of the DHA. The ACSC is now limited to providing "advice and support" to both the government and nongovernment actors on cybersecurity (ACSC, n.d.). For example, the Critical Infrastructure Centre was established in 2017 within the DHA to protect Australia's critical infrastructure from any form of interference or sabotage from foreign actors (Cyber and Infrastructure Security Centre, 2021).

Finally, the ambassador for cyber affairs under DFAT is responsible for promoting the country's cybersecurity interests abroad. This involves coordinating with both foreign governments and businesses to secure Australia's security, economic, and development interests "in cyberspace and critical technology" (DFAT, n.d.) as set in the National Cyber Security Strategy. Other departments of the Australian government serve a smaller role translating cybersecurity goals into appropriate programs for their mandate. For instance, the minister of communication is focused on online safety and consumer safeguards, while the minister of industry is involved in building the country's domestic cybersecurity industry through its cybersecurity industry growth center, AustCyber. The minister of education, through the Department of Education and Training, implements a program to encourage more students to study cybersecurity and related courses (Department of Industry, Science, Energy, and Resources, 2018).

Legal Framework

The following laws are integral to Australia's robust cybersecurity legal framework:[2]

- Criminal Code Act 1995 (as amended by the Cybercrime Act 2001)
- Telecommunications (Interception and Access) Act 1979
- Spam Act 2003
- Telecommunications Act 1997
- Privacy Act 1998
- Security of Critical Infrastructure Act 2018

- Surveillance Devices Act 2004
- Intelligence Services Act 2001
- Australian Security Intelligence Organisation Act 1979

The Amendment to the Telecommunications Act of 1979 was introduced through the Telecommunications and Other Legislation Amendment (Assistance and Access) Act of 2018. The reforms enabled law enforcement agencies to effectively tackle online criminals by improving legitimate computer access powers and enhanced cooperation with industry players (Parliament of Australia, 2018).

The Australian government is examining reforms to current legislation to "set a minimum cybersecurity baseline across the economy" (DHA, 2020a, p. 22). Reform areas include privacy, consumer, and data protection laws and obligations on manufacturers of Internet-connected devices (DHA, 2020a). In addition, it is exploring how legislation can support private sector initiatives to protect citizens and businesses (Penn, 2020).

Toward the end of achieving a minimum level of cybersecurity across the entire nation, there are ongoing discussions on amending the Security of Critical Infrastructure Act of 2018 to enhance the regulatory framework and broaden the scope of critical infrastructure, with the effect of requiring certain security standards to be met across a wider range of industries. In addition to electricity, gas, water, and ports, the amendments would include the following:

- Communications
- Financial services and markets
- Data storage or processing
- Defense industry
- Higher education and research
- Energy
- Food and grocery
- Healthcare and medical
- Space technology
- Transport
- Water and sewerage

Current Cybersecurity Strategies

The Department of Home Affairs, the main agency in charge of cyber policy, led the development of Australia's 2020 Cyber Security Strategy. Prior to the DHA's establishment, the Strategy was developed by the Attorney General's Department (for the first edition, in 2009) and by the Department of Prime Minister and Cabinet (for the second edition, in 2016).

With a development budget of AUD 230 million, the 2020 Strategy sets out to achieve the vision of “a more secure online world for Australians, their businesses and the essential services upon which we all depend” (DHA, 2020a, p. 4). The Strategy puts a strong focus on shared responsibility among government, businesses, and community, and sets out key action themes for them to commit to undertake to deliver the vision.

The 2020 Strategy was developed using a consultative process led by the DHA, emphasizing the importance of a “national cyber partnership” that brings together all sectors of Australian society. This process included the establishment of an industry advisory panel to ensure that industry advice and support are taken into consideration in the development of the Strategy.

The new strategy represented a significant development from the 2016 edition, from a primarily reactive cybersecurity posture to a proactive one. The 2016 strategy, which established the ACSC and appointed the ambassador for cyber affairs, focused on reacting to developing threats to Australia’s networks and systems. One criticism of this previous document was that it aimed to achieve a poorly defined “open, free, secure” Internet (Stilgherrian, 2019a).

For 2020, the government had committed to invest AUD 1.67 billion over the next 10 years, a more than 600% budget increase from the previous edition. The 2020 edition of the document also lays out a 10-year plan for the country, whereas the previous edition only covered 5 years—signaling a more long-term vision for Australia’s cybersecurity.

A significant portion of the budget goes to ACSC mainly to build capacity both within and outside the government, build more partnerships, and protect Australians. The ASD will employ an additional 500 cyber personnel over the next 10 years as part of this action. An expert noted the strong focus on domestic cybersecurity, strengthening law enforcement and protecting Australians online in the 2020 Strategy (Uren, 2020).

The government will commit funds to enhance existing Joint Cyber Security Centres to support stronger partnerships between businesses and state/territory governments. The Strategy also includes a program to assist small and medium enterprises to uplift their cybersecurity through tailored advice and assistance. In addition, the Strategy outlines programs to support businesses and the academe in growing a cyber-skilled workforce and promoting innovation in cybersecurity research and development through AustCyber.

In April 2021, the government launched the Cyber and Critical Technology International Engagement Strategy, which will guide Australia’s practical international engagement across cyber and critical technology issues. Its key objective is to “strengthen national security, protect Australia’s democracy and sovereignty, promote economic growth, and pursue international peace and stability” (Payne, 2021).

While Australia’s cybersecurity posture is anchored on democratic values and promotes a multistakeholder approach, some policy and government actions have raised concerns about their impact on the openness of the Internet. As a long-standing member of the Five Eyes intelligence alliance,[3] Australia has been a proponent of monitoring Internet traffic, breaking encryption protocols, and installing backdoors for government access in networks and systems (Scroxton, 2020). Outside of this alliance, Australia has also moved to reduce certain Internet freedoms, such as by deanonymizing trolls on social media platforms, in the name of national security (Keith, 2021).

Australia, along with the rest of the Five Eyes, have shown a willingness to engage in offensive cyber activities to deter threats. The 2016 Cyber Security Strategy acknowledged Australia's offensive cyber capabilities (OCCs), with no less than then-Prime Minister Malcom Turnbull arguing that it is an important deterrent against destructive attacks for which defensive tools alone would not suffice (Gold, 2020). The government has acknowledged that both the ASD and the Australian Defence Forces have OCCs and that they have been used against various targets, including the Islamic State, foreign cybercriminals, and more recently, entities involved in COVID-19-themed attack campaigns.

Australia has stated that it only uses OCCs in a manner that is targeted, proportionate, subject to legal oversight, and consistent with domestic and international legal obligations (Gold, 2020). It also released a 2017 International Cyber Engagement Strategy outlining specific policies for the use of OCCs in military operations. Among the Five Eyes countries, Australia has been among the most vocal about government transparency on OCCs, something it has used to publicly reconcile its offensive capabilities with its commitment to a safe Internet. The Australian government has also called on other countries to be similarly transparent on the development and use of OCCs in a manner consistent with international norms.

Key Takeaways

Both Australia's cybersecurity governance structure and the Cyber Security Strategy 2020 show a commitment to a democratic, multistakeholder-driven approach to a shared national vision for cybersecurity. The involvement of multiple departments in differing areas of cybersecurity policymaking and implementation, far from hindering the formation of a coherent strategy, has created a high level of cyber risk awareness throughout the government. This avoids the problem of cybersecurity being a silo issue for only one government body. Combined with Australia's financial commitments to cybersecurity, this has given the country a strong defense, making it a harder target for increasingly frequent and sophisticated cyberattacks. Although the Australian government recognizes that there is still much to be done, it has made significant progress in building trust and security in Australia's digital economy since cyber threat was first recognized as a national security concern. The World Economic Forum has rated Australia as among the most prepared when it comes to an attack (Santiago, 2015). The country also ranked 11th in the world and 3rd in the Asia Pacific region in the 2018 Cybersecurity Index and achieved the maximum score for its legal and organizational pillars (ITU, 2019).

Several insights on cybersecurity governance can be gleaned from the successful ongoing development of cybersecurity policy in Australia. These include the following:

- **Executive sponsorship.** The prime minister himself articulated the gravity of the program and the need to have a systemic solution for it. The policy move from the Attorney General's Department to the DHA was also a push upward. Since 2009, cybersecurity has remained an important agenda item for Australia, as shown by the number of information security laws they have in place and the increasing public investments to enhance its cyber intelligence capabilities.
- **Cross-agency and multistakeholder collaboration on cybersecurity policy development and implementation.** With the creation of the DHA, and the Cyber Security Policy Division under it, Australia has institutionalized a whole-of-society approach to cybersecurity that values input from stakeholders in the public and private sectors, civil society, and the academe. Moreover, by delegating implementation responsibilities among the DHA, Department of Defense, DFAT, and other government offices, Australia has helped develop shared responsibility and ownership for cybersecurity. Supporting this is a strong push to develop cybersecurity capacity across all sectors of society and a structure for coordinating cybersecurity activities so that they are harmonized with the national strategy. This could be adapted in a country such as the Philippines through the establishment of a national cybersecurity coordination bureau.
- **Joint Cyber Security Centres program.** The creation of hubs allows each federated state to own their cyber posture and build capabilities but still be centralized. This program can be likewise implemented in urban centers of the Philippines that have significant cyber capabilities.
- **Strong dedicated focus on critical infrastructure.** Australia's Parliament passed the Security of Critical Infrastructure Act of 2018 and created a separate and dedicated government agency for this.

China

China's exponential growth has been driven in part by its rapid shift to the digital economy. This transformation is seen in the state's use of information technology as a vital tool of governance. In the private sector, China is one of the world's largest investors and adopters of digital technologies and is home to one-third of the world's unicorns, or startup enterprises with valuations of USD 1 billion and above (Woetzel et al., 2017). Even before the pandemic, China's digital economy was already worth an estimated USD 4.7 trillion or 34.8% of the GDP (Jun, 2020).

Within this context, the CCP views the protection of its digital infrastructure through cybersecurity as a national priority (Gierow, 2014). The Chinese government has two major levers when it comes to enforcing security via digital means: legal traffic interception and censorship. One of the most iconic manifestations of censorship is the "Great Firewall of

China." The government also asserts control over the population through digital mechanisms like credit scores that rate a person's compliance with local laws. China's economy relies on digital payments, which, in cities like Shanghai, have replaced cash as the primary means of transaction. In the realm of national security, these digital command and control systems are also responsible for coordinating military activity and allocating resources. Computer systems protect vital state secrets from being leaked. Overall, a compromised digital space undermines the effective functioning of the state.

Cybersecurity Governance and Legal Framework

China's cybersecurity governance has been constructed as a means of promoting Chinese national interests. Because an increasing amount of daily life is mediated online, China's control of the Internet helps demonstrate its sovereignty over the population. Through passing cybersecurity laws, China can project its competence in complying with global standards for digital security.

China's cybersecurity framework is primarily outlined in the Cybersecurity Law of 2016. Before its passing, regulations on digital security were scattered throughout various laws and ordinances. The 2016 law provides cohesion and a unifying framework to the various protocols in place. The law applies to two important stakeholders: network operators and critical information infrastructure (CII) operators. Network operators are widely construed to refer to any businesses that own or operate their own local networks in China. CII operators, on the other hand, cover firms that operate in industries that are deemed critical by the government.

One salient feature of the law is a requirement for network operators and CIIs to store existing customer data in local servers, effectively banning these firms from exporting data abroad (Wagner, 2017). Another important provision requires firms to actively cooperate with the government in investigations relating to data breaches. These firms are compelled to give the government access to their data for purposes of national security. The law widely encompasses several aspects of cybersecurity and has provisions on areas such as protocols for the collection of private information, mandates for the development of internal cybersecurity systems, regular conduct of security assessments and drills, and minimum reporting standards for compliance agencies (Wagner, 2017).

The Cybersecurity Law must also be considered alongside the National Intelligence Law of 2017, which strengthens the presence of the Chinese government in the private sphere. One of this law's primary mandates compels citizens to actively cooperate with the state in intelligence-gathering efforts. Article 7 of the National Intelligence Law states that "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law" (National People's Congress, 2017). The provision, phrased as a general mandate, prescribes no limits on the extent to which China can compel companies to turn over private information. This can potentially affect Chinese entities that operate overseas.

States usually justify intrusions on private liberties as a means of averting greater dangers, including threats to national security. In contrast, the National Intelligence Law fails to state a national security justification for government intrusion. Instead, Article 14 of that law gives the government the absolute authority to “demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation” (National People’s Congress, 2017). These gray areas in legislation provide wide latitude for the CCP to make the rules as they go. The government utilizes a strategy of introducing more draconian measures to original legislation, making it much more restrictive than originally conceived. This reduces the barrier to legally compelling Chinese individuals and companies to obtain information or act on behalf of the CCP.

Three years after its passing, the Cybersecurity Law has been plagued with issues of enforcement and compliance. Several firms have complained that certain recommendatory guidelines on the collection of customer information are made mandatory in practice (Rechtschaffen, 2019). There is also considerable vagueness in how the law applies to sectors such as medicine, where there are no specifications as to what details in a patient’s medical history can be collected. The level of arbitrariness has caused some foreign technology businesses to leave China; the lack of clarity has made it harder to do business as firms increasingly run into conflict with regulators who can impose hefty fines.

Promoting Chinese National Interests

The Chinese framework differs starkly from that of its Western counterparts. One salient feature of the Chinese cybersecurity paradigm is the relative absence of protections for privacy that are present in Western frameworks. In European states, privacy is integrated as a fundamental right that must be preserved in the digital sphere. In the United States, privacy is viewed more as a consumer right for clients or purchasers of products and services. Both treatments of privacy are rooted in the individual’s consent as a prerequisite for accessing personal data and information.

In contrast, the Chinese framework places paramount importance on the ability of the state to provide social order. China’s surveillance infrastructure was created with the goal of monitoring individual behavior to determine the degree to which citizens comply with social norms. China deploys surveillance cameras along major streets and thoroughfares to identify those who violate pedestrian laws. Its online database and social credit system for civilians enable the creation of a system of social incentives and penalties for behavior. What these measures achieve is ultimately the maintenance of national security. Through the digital sphere, China enhances its ability to influence citizens’ behavior even without physical force. Subsequently, China’s control over its largest digital companies allows them to ward off external threats. The deployment of 5G networks in neighboring countries by firms such as Huawei allows China to export its surveillance and security features abroad.

China's domestic cybersecurity framework brings certain dangers to the rules-based international order. As demonstrated, the Chinese government's complete access to the data of its local network providers constitutes a security threat to nations whose companies do business with these firms. The framework also undermines individual liberties on a massive scale. Both cybersecurity and intelligence laws set legal cover for state surveillance over the population.

China today uses information systems to monitor citizens' behavior, utilizing data and metrics to quantify social compliance. The burden of proof that the government needs to access confidential data is low; intelligence can be gathered even for cases where there are no urgent risks to national security. These dangers outline the Chinese system of governance built on principles in conflict with that of other nations.

Key Takeaways

One approach to Internet governance views effective information systems as top-down enterprises where the state has direct control of the digital sphere (Rosenbach & Chong, 2019). The other advocates for the bottom-up development of information security through competition and open access between different players. An analysis of the Chinese framework shows that dealing with policy issues in cybersecurity requires an engagement with these broader questions of competing principles.

China's cybersecurity posture also poses grave concerns for countries such as the Philippines with whom it may have conflicting claims. The Chinese government has increasingly resorted to soft power to influence other countries, to the extent that it could compromise other countries' cybersecurity posture. Projects such as telecommunications infrastructure deployments, which entail the use of Chinese technologies and equipment, potentially give China unique access to sensitive information within other countries.

Israel

Israel has been in constant conflict and tension with its neighboring states since it declared independence in 1948. It has successfully defended against attempted invasions by some of its neighbors in the Middle East. Naturally, national security and defense has always been a strategic focus of the Israeli government, cybersecurity included.

Israel's cyber resiliency is regularly tested by bad actors. Since the 2010s, there have been tit-for-tat cyberattacks between Israel and Iran (White, 2020). During the 2014 Gaza War, Israel revealed that its government, military, and economic sites were persistently targeted by actors linked to Iran (Opall-Rome, 2015). In 2020, Israel uncovered a series of cyberattacks on its water systems (Cimpanu, 2020c). Not long after, Iran's busy Shahid Rajee Port suffered an attack that damaged its computers, targeting electronic infrastructure to disrupt the flow of goods (*The Times of Israel*, 2020). A series of blasts in critical Iranian sites have also been linked to the United States or Israel. These events illustrate how the rivalries of nation-states in the physical world are now manifested in cyberspace, sometimes even targeting civilians (Fassihi & Bergman, 2021).

Today, Israel is considered one of the global leaders in cybersecurity, which gives it both military advantage and economic edge. As of 2019, Israel has exported cybersecurity solutions totaling USD 7 billion, with close to 10% of the global market share (Reuters, 2019). It has successfully created a cyber-ecosystem with an innovative and thriving private sector, universities, research laboratories, military intelligence units, and widespread government support (Raska, 2015).

Legal and Governance Framework

The constant threat imposed by its neighbors has shaped the evolution of Israel's cybersecurity framework. As early as 1997, Israel set out to protect its critical infrastructure through the creation of the Tehila Unit, in charge of coordinating state information and communications technology (ICT) infrastructure.

In 2002, the government authorized the National Information Security Authority to instruct and protect vital computer systems of key public and private sector organizations, or critical infrastructure.

Over the years, the Israel Defense Forces (IDF) has been mainly responsible for the country's cyber sphere with permanent units for both cybersecurity and cyber defense. For example, the IDF's Unit 8200 is responsible for offensive cyber operations, having been linked to the intelligence collection initiative known as Flame in 2012 and the disruption of Iranian nuclear control systems through the Stuxnet worm. The C41 Directorate, on the other hand, is responsible for protecting IDF's ICT communication infrastructure and systems. It is also responsible for deterring and preempting attacks on the country (Raska, 2015).

In 2011, there was a notable shift in Israel's cybersecurity focus when Prime Minister Benjamin Netanyahu (2009–2021) declared his vision of Israel as among the top five countries in the world in terms of cybersecurity. The country expanded its strategy to protect not only critical infrastructure but also the civilian and private sectors. In 2011, the government issued Resolution 3611 on Advancing the National Capacity in Cyberspace.

In 2012, the Israel National Cyber Bureau was established as part of the Prime Minister's Office. It was tasked to establish the country's national cyber policy and strategy, promote national processes, develop national cyber capabilities, and strengthen Israel's leadership in cyberspace (National Cyber Directorate, 2017).

In 2015, the government issued two resolutions: (1) Advancing the National Preparedness for Cyber Security, which established the National Cyber Security Authority, tasked to lead the country's operational cybersecurity efforts (Resolution 2444); and (2) Advancing National

Regulation and Governmental Leadership in Cyber Security (Resolution 2443). The Israel National Cyber Bureau and the National Cyber Security Authority make up the Israeli National Cyber Directorate (INCD) (National Cyber Directorate, 2017). As one of only four agencies directly under the Prime Minister's Office, the INCD is responsible for strategic policy planning, national-level implementation, and facilitation of international coordination in cybersecurity.

In 2017, the current Israel National Cybersecurity Strategy was formulated. It outlines the priorities and goals of the INCD: to defend Israel's economic and social strength, institutionalize capacity building, and strengthen international cooperation (Frei, 2020). Most cybersecurity directions are led by the IDF and INCD. Based on the NIST Cybersecurity Framework, the Israeli framework focuses on robustness, resiliency, and defense.

Cybersecurity Ecosystem in Israel

Israel's determined focus to be a global leader in cybersecurity has translated into government programs and funding for a thriving cybersecurity landscape. Although rooted in a strong military and defense rationale, it is now a successful nationwide ecosystem and an integral part of the Israeli economy. Aside from consistent government spending and focus on cybersecurity, other factors that sustain this include a targeted investment in human capital and a thriving private sector.

Valuable Human Capital

Israel has a 24- to 30-month mandatory[4] military service for both Israeli women and men, exposing young Israelis to cutting-edge technological innovations in cybersecurity, which has led to a vibrant cybersecurity market.

The Israeli government offers an Academic Reserve program, where the top 1% of high school graduates are offered scholarships to complete their science and technology degrees, or other degrees deemed critical by the IDF, before completing their military service (Bagram & Ben-Israel, 2019, p. 77). The scholars subsequently serve an additional 3 to 5 years should they choose to serve in IDF technological units. This system provides a constant pool of knowledgeable and professional Israelis serving the government. Talpiot, a subprogram of the Academic Reserve, offers an elite 40-month training program on IDF-identified critical degrees and military courses (Bagram & Ben-Israel, 2019, p. 84). Talpiot participants also serve six additional years in the IDF. After the compulsory service, graduates of the Academic Reserve may choose to pursue a military career or a civilian career, strengthening the country's cybersecurity position either way.

This education and training strategy is not only focused on the military; it is also present in mainstream basic education. In middle school, cybersecurity is offered as an elective (Press, 2017). In some schools, students learn computer programming as early as fourth grade, and encryption as early as tenth grade (Estrin, 2017). In Tel-Aviv University, non-arts university degrees all have a cybersecurity specialization. Six university research centers, headed by Academic Reserve graduates as of 2018, are dedicated to cybersecurity (Bagram & Ben-Israel, 2019).

Thriving Cybersecurity Market

With 436 active cybersecurity firms spread throughout the country, Israel tech firms raised USD 9.3 billion of private investment in 2020 (Solomon, 2020). With a strong incubator and innovator environment, startups sprout each year, whereas some are focused on growing through mergers and acquisitions. Israel has also been called “startup nation” because it has the largest number of startups in relation to its population size (Yerman, 2019). In 2020, venture capital funding raised USD 2.7 billion with most capital going to growing existing companies. The average venture capital deal has also increased from USD 3.3 million to USD 5.2 million from 2017 to 2020, showing a consistent upward trend (Dov, 2021).

Israel has also set up Advanced Technologies Park (ATP), a public–private partnership that promotes technology and commercialization of cutting-edge research and innovation (Ben-Gurion University of the Negev, 2013). Located beside Ben-Gurion University, which boasts of a cybersecurity research center and advanced degrees in cybersecurity, ATP is meant to be an innovation and collaboration hub for the academe, the private sector, and the military. ATP offers an array of incentives to attract companies, including tax exemptions for 10 years, accelerated depreciation, and grant assistance (Ben-Gurion University of the Negev, 2013). The park has attracted successful companies such as Microsoft, Intel, HP, Google, Deutsche Telekom, PayPal, Dell EMC, IBM, and Oracle. Venture capitalists, research laboratories, startup businesses, and other technologically related enterprises have also moved to ATP. IDF’s information technology (IT) units are also expected to occupy a third of the park (Press, 2017).

Israel’s status as one of the leading lights in cybersecurity is perhaps marked by its international cybersecurity cooperation agreements with traditional world powers, such as the United States, Australia, and Japan.[5]

Key Takeaways

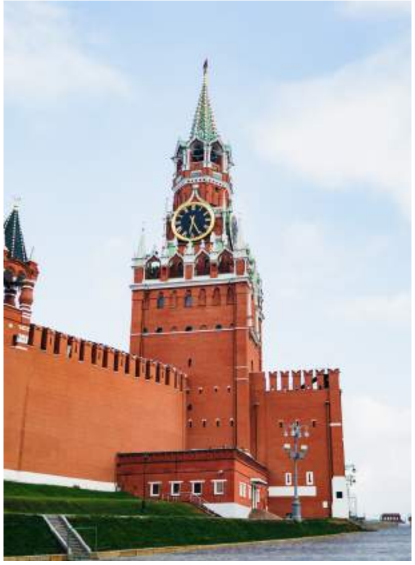
The geopolitical realities of Israel have led to its mature security posture. The past decades have shown an expansion of cybersecurity focus from protection of critical infrastructure toward involvement of the private sector, and from cybersecurity handled solely by IDF and INCD toward a whole-of-society approach.

The shift of cybersecurity as a purely military and national security realm to an economic growth driver has made its current cybersecurity ecosystem thrive. Israel still receives various cyberattacks, and allegedly targets others, but its security position is recognized as one of the best in the world.

There are some policy lessons that other nations can learn from the Israelis:

- **Creation of an academic program that allows the best of the best to work in key focus areas.** The Academic Reserve is an interesting model that could be used to create a sustainable pool of talent for industries like cybersecurity. Countries such as the Philippines might even be in a better position to execute this due to our larger workforce base. Of course, support for cyber programs in academic institutions can also further feed into this program.
- **Alignment toward the military and law enforcement.** This is one of the key aspects of the Israeli experience, with both defensive and offensive capabilities built in support of military goals. Even nations that do not face the same intense existential threats as Israel should be prepared for external threats from other states that would traditionally call upon a military-based response. Addressing cybersecurity threats may require military-aligned, or at least law-enforcement-aligned, capabilities.
- **Executive-level sponsorship.** Israeli cybersecurity programs are driven by the mandate of the heads of government. Successful national cyber programs should likewise derive their mandate from the highest possible executive authority.

Russia



Having been the United States' major rival in the Cold War, Russia continues to see itself as a superpower that can heavily influence world affairs. This historical backdrop informs how Russia has shaped its cybersecurity regime. It explains Russia's legal frameworks for upholding the security of its agencies, as well as assets to be used in the context of warfare. During the Cold War, the United States and Russia contended for power through civil conflicts in developing nations. Each state would back opposing factions in civil wars, often providing resources and funding. Even without overt war, the two superpowers proved able to destabilize other nations by delegitimizing the popularly elected leaders. That geopolitical backdrop is still relevant to the promotion of Russian national interests and informs the role of cybersecurity and information security more broadly.

Structure of Russian Cybersecurity Governance

Russian cybersecurity governance consists of both institutional and legal structures aimed at protecting its critical infrastructure, as well as methods for improving its offensive capabilities. The origins of these institutional structures can be traced to policy pronouncements, memos, and other documents containing Russian state policy. Pronouncements by top Russian leadership are codified by security agencies into policy documents that lead to the development of more cohesive cyber strategies.

Some critical junctures in the development of Russia's cybersecurity frameworks include the 2003 joint session between Russian Security Council and the State Council, where President Vladimir Putin (2000–present) raised the urgency of creating a national policy toward objects critical to national security and their protection from human-made, natural, and terrorist threats (Pursiainen, 2021). Another important event was the 2014 Russian annexation of Crimea,[6] which was followed by the enactment of laws, ordinances, and internal policies related to the protection of Russian critical infrastructure to mitigate any retaliation from hostile states (Iasiello, 2017).

Within these wide-ranging policies, efforts can be traced to categorizing "critical information objects" (particularly, as "critically important" vs. "potentially dangerous"). Other laws, such as a 2012 document from the Russian Ministry of Emergency Situations, offer a methodology for classifying objects based on threat source (particularly, attacks to state organs and key sectors).

These frameworks define both the defensive and offensive aspects of Russia's cybersecurity operations. Russia's *defensive* cybersecurity posture relies on a broad conception of where threats originate. Aside from terrorist attacks, Russian proclamations also identify threats from local opposition groups, foreign state actors, and natural disasters (Pursianen, 2021). Principles of Russia's *offensive* cyberattacks also underlie its defensive posture. In response to threats, power is vested in a direct and hierarchical fashion to state authorities who are responsible for fortifying critical infrastructure. There has been greater urgency for Russia to focus on its defensive systems to mitigate the threat of retaliation for recent attacks that were allegedly state sanctioned.

Besides the protection of critical infrastructure, Russian cyber governance also emphasizes the development of the nation's offensive capacities. There are two primary agencies in Russia that handle matters relating to information systems, intelligence, and cyber warfare: the Federal Security Service of the Russian Federation (FSB) and the Main Directorate of the Armed Forces of the Russian Federation (GRU).

Throughout the early 1990s to 2000s, the FSB oversaw cyber operations in the burgeoning Internet landscape (Lilly & Cheravitch, 2020). It pursued informal relationships with programmers and hackers to conduct operations on behalf of the agency. No cohesive cybersecurity program existed at the time. The loose coalitions carried out cyberattacks in Balkan states such as Estonia and Georgia to invalidate governments critical of Russian hegemony (Lilly & Cheravitch, 2020). Most of these operations were relegated under the general intelligence or espionage work of the Russian state.

A more cohesive cyber warfare program started in 2013 under the GRU. While the FSB acts as the state's central intelligence agency under the control of the president, the GRU is the military's main intelligence unit. After getting the endorsement of the president, the GRU launched a big hunt for programmers to fill its units created for cyber research and development (Lilly & Cheravitch, 2020). The Russian Ministry of Defense subsequently announced the launch of an information operations force that would carry out programs designed by the new research centers. What made GRU programs distinctive was the aggressiveness of the attacks launched. Intelligence work had previously focused on defensive capabilities and informational advantage for a country; the cyberattacks developed within the GRU focused on dismantling foreign information systems.

Strategic Basis for Russian Cyber Offense

There are several advantages of cyber operations as a tool of warfare. Several global conventions exist that guide state actions in case of military conflict. These codified rules and procedures outline the permissible responses states can take when physical attacks are launched. In contrast, global rules and norms relating to cyberattacks are much more ambiguous. A cyberattack fails to meet the threshold for constituting an act of war. At the same time, it is not as easy to quantify the damage done by a data breach compared to the loss of human life or infrastructure in a physical conflict. The gray area benefits states that sponsor cyberattacks in that the lack of rules allows them the flexibility to conduct these operations while still engaging with nation-states through diplomatic channels.

Several agencies and government research firms in other countries have drawn links between operations by Russian-based hacking groups and directives from the Russian government (Roth, 2021). Activities that have been connected to Russian-based cyber actors include disinformation campaigns in other countries and hacking of state servers and digital systems (Lysenko & Brooks, 2018).

A prime example of such campaigns is the alleged efforts by Russian state authorities at disinformation in the 2016 U.S. elections (Mueller, 2019; U.S. Senate, 2018). A Russian firm called the Internet Research Agency, also known as Glavset, has been linked with the creation of a large troll farm that created thousands of social media accounts supporting far-right causes (Lapowsky, 2017). These fake accounts supposedly of American citizens bolstered the campaign of Donald Trump and smeared the candidacy of Hillary Clinton. Also, computer hackers were able to infiltrate the computer systems of the Democratic National Committee and subsequently released thousands of leaked emails through sites such as Wikileaks (Lipton et al., 2016). The example of election interference shows not only the diversity in Russia’s efforts but also their competence in employing these techniques. In 2020, a major Russian-orchestrated cyberattack was uncovered by U.S. intelligence agencies. The breach was committed by a hacking group called Cozy Bear, which was backed by the Russian government agency SVR (Vavra & Starks, 2020). It was found that the attack affected thousands of organizations, including critical government agencies in the United States such as the Treasury Department, the National Telecommunications and Information Administration, and part of the Department of Commerce.

Amid the perception that its government is actively involved in sponsoring cyberattacks, Russia effectively denies any accusations that tie the government to cyberattacks by Russian-based hackers. The lines between acts of the Russian state and criminal behavior by Russian agents are at times not easily demarcated. In previous incidents, the Russian government would deny and/or deflect any accusations tying it to digital attacks against Western government agencies. It would then divert blame back to the United States and western

European countries, claiming that they are the purveyors of the practices they accuse Russia of doing (Tidy, 2021). It must also be noted that this cyber offense tactic is also employed by other nations, but they, naturally, publicly deny responsibility for any attacks.

Key Takeaways

The coherence in Russian cybersecurity policy lies in an understanding of the evolving nature of conflict and warfare. Some research institutions and government agencies in other countries have drawn a link between recent cyberattacks and the Russian government, including officials in the highest rung of the state's intelligence agencies. These agencies, particularly the GRU, have reportedly openly recruited programmers and have set up subdepartments for the advancement of cyber capabilities.

Russia's cybersecurity landscape focuses on the development of defense capabilities as well. Laws and ordinances have been enacted to define critical infrastructure and classify threat sources. Like other countries, Russia can be expected to continue developing these capabilities in the next few years.

Given the aggressiveness of states such as Russia in cyber offense, the lack of a global governance framework on cybersecurity compromises the collective security of all nation-states. Dealing with such states necessitates nations to focus not just on the defensive side of information security but also on offensive information security capabilities. The concept of "know thy enemy" comes to mind. This can potentially provide insights on the latest threats while keeping us sharp with better practice and drills. Active vulnerability-hunting activity is also a good use of this offensive capability.

United States

Cybersecurity has considerably grown as one of the most critical issues confronting the U.S. government's national security agencies. This has mostly been due to the growing dependence on the Internet and computer-based systems and transactions. These have contributed to the vulnerabilities of American companies and government agencies to cyberattacks. In April 2015, for example, millions of sensitive personal data were hacked from the U.S. Office of Personnel Management; the hack was linked to state-sponsored attackers working for the Chinese government (Gootman, 2016). This incident, however, was just the tip of the iceberg as there have been numerous cyberattacks and breaches against U.S. businesses and government agencies in recent years, including the National Nuclear Security Administration, Department of State, Department of Homeland Security, and the Department of Defense, among others. In 2020, the Cyber Risk Index listed the United States among countries most vulnerable to cyberattacks. Due to the U.S.-led War on Terrorism, Americans have also been among the primary targets of cyberterrorists around the world.

In understanding the U.S. security strategy, we must look at it from several angles, including the current strategic environment in which the world is conflictive and dominated by states.

The challenges to American security interests do not necessarily assume traditional forms (i.e., militaristic approaches), given the increasing reliance of warfare methods on cyber operations (Lewis, 2020). The U.S. cybersecurity policy operates within this novel strategic context in which there is an increasing role for states in cyberspace and digital platforms. In this regard, it is important to examine the interplay between cybersecurity and the broader U.S. national security policies.

Legal and Governance Frameworks

During the Obama administration (2009–2016), a survey from the *Defense News* indicated that over 45% of the U.S. national security leaders identified cyberwarfare as the most pressing danger to the country (Pizzi, 2014). Former Homeland Security Secretary Janet Napolitano warned that a "cyber 9/11" is a looming threat and could target critical infrastructure, including water and electricity (Reuters, 2013).

President Barack Obama (2015) outlined four basic principles in addressing cybersecurity threats. First, he emphasized that resolving cybersecurity threats is a "shared mission" requiring the joint efforts of the government and the private sector. He also underscored the need to focus on combining the "unique strengths" of government units and businesses in coordinating a response that cuts across different companies and sectors. The country should "constantly evolve" given the growing sophistication of cyberattacks. Lastly, he stressed the need to protect the privacy and civil liberty of Americans.

These fundamental principles were embedded in Executive Order (EO) 13691 s. 2015, which aims to encourage and promote cybersecurity threat-information sharing within the private sector. It was also envisioned to draw upon EO 13636 s. 2013 (Improving Critical Infrastructure Cybersecurity) and the Presidential Policy Directive-21 (PPD-21) of 2013 (Critical Infrastructure Security and Resilience). Under these executive issuances, the U.S. government's primary goal is to increase its defense capabilities against cyberattacks by improving information sharing, securing privacy, and following best practices. Previously, the U.S. government also instituted the following initiatives to combat cyber-related threats: the National Infrastructure Protection Plan Update (U.S. Department of Homeland Security, 2009); Whitehouse Cyberspace Policy Review (National Security Council, 2009); and the National Strategy for Trusted Identities in Cyberspace (The White House, 2011).

Under EO 13636, President Obama requested the establishment of a cybersecurity framework. In response, the National Institute of Standards and Technology consolidated the best practices in information sharing from the private sector and used the following steps in developing the U.S. National Cybersecurity Framework (NIST, 2018a):

1. Identify (assist in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities)
2. Protect (outline appropriate safeguards to ensure delivery of critical infrastructure services)
3. Detect (identify the occurrence of a cybersecurity event)
4. Respond (take action regarding a detected cybersecurity incident)
5. Recover (maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity incident)

In line with the U.S. Cybersecurity Framework, the Joint Task Force introduced the NIST Special Publication (SP) 800-53[7] to develop the standards and guidelines to recommend the manner the U.S. government agencies are able to implement and supervise their information security systems. NIST SP 800-53 established a cohesive information security structure that encourages proactive risk control through the federal government. The NIST SP 800-37 focuses on the following control families (classified as low, moderate, and high): access control, audit and accountability, awareness and training, configuration management, contingency planning, identification and authentication,[8] incident response, maintenance, media protection, physical and environmental protection, planning, program management, risk assessment, security assessment and authorization, system and communications protection, system and information integrity, personnel security, and system and services acquisition.

In addition, the Obama administration implemented the Federal Information Security Modernization Act of 2014 (FISMA Reform), which is an amended version of the 2002 legislation, in response to the growing number of cyberattacks against the federal government.

In 2015, the United States and China signed a bilateral agreement to avoid economically motivated cyber espionage between the two countries, especially in the areas of trade secrets and intellectual property theft. The agreement attempted to increase the level of engagement between the two countries and decrease the number of attacks against U.S. companies. There have also been different bills filed in the U.S. Congress on cybersecurity and information-sharing practices. During the 114th Congress, the following relevant bills were introduced: Cybersecurity Information Sharing Act of 2015 (S. 754); Protecting Cyber Networks Act (H.R. 1560); and National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731). Under these laws, the government underscored the need to follow a “whole-of-government approach” in combating cybersecurity threats while protecting the civil liberties of Americans.

Response to Active Cybersecurity Threats

There has been an increasing range of cybersecurity-related issues confronting the United States. While the Obama administration sought a more legalistic approach, the Trump administration (2017–2021) enforced more aggressive steps in tackling cyber-related threats. Before the 2016 U.S. presidential election, two fundamental issues occurred. First, there was the theft of emails of the Democratic National Committee by the Russian military intelligence agency GRU, which purportedly operated under the direction of Russian President Vladimir Putin. These leaked documents reportedly helped the electoral campaign of Donald Trump (Nakashima & Harris, 2018). Second, there was also an increased use of social media to foster dissension and polarization among the public. A Russian troll farm, identified as the Internet Research Agency, used divisive issues in the country (e.g., racial discrimination, gun ownership) to inflame public sentiment. This Russian troll farm bought Facebook advertisements to disguise as grassroots organizations, mobilize rallies, and undermine the integrity of U.S. democratic processes (Rodriguez, 2019).

Such incidents have made the U.S. government more cautious and vigilant of cyber-enabled and cyber-dependent foreign interferences. There are a few key points regarding the response of the United States to cyber espionage. The American government, for example, has implemented a set of technical testing for election tools to encourage all state and local officials to use multifactor authentication. In addition, those who were caught actively interfering in the election were sanctioned. In 2018, the U.S. Department of Justice charged 12 Russian intelligence officers with hacking the accounts of Democratic officials in the 2016 U.S. elections (Tucker, 2018). In addition, there was also an acknowledgment among social media corporations (e.g., Facebook and Twitter), who have massive influence on elections and political discourse, about the need to address the issue of fake news and disinformation by working with the government.

The enactment during the Trump administration of the John S. McCain National Defense Authorization Act (NDAA) of 2019 allowed for a more detailed and comprehensive budget allotment for strategic programs and assessments related to the U.S. policies on cyberspace, cybersecurity, cyber warfare, and cyber deterrence. President Trump also issued EO 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure due to the security risks of cyberattacks on critical infrastructures. In enhancing the cybersecurity capacities and capabilities of the U.S. military, some of the highlights of President Trump's cyberspace policy include turning the Cyber Command into a unified combatant command through the establishment of the Cybersecurity and Infrastructure Security Agency (CISA). CISA coordinates the execution of the national cyber defense in partnership with the Office of Management and Budget (the agency responsible for overall federal cybersecurity). CISA is also responsible for sharing timely and actionable information across government and private sector partners.

For years, the approach of the Department of Defense (DOD) to cybersecurity has been focused on defending U.S. digital infrastructure. The 2018 DOD Cyber Strategy directed the department to "defend forward," shape the day-to-day competition in cyberspace, and prepare for war. *Defend forward* means to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." *Taking action in cyberspace during day-to-day competition* means to "preserve U.S. military advantages and to defend U.S. interests by focusing on "states that can pose strategic threats to U.S. prosperity and security, particularly China and Russia." *Preparing for war* means that the US cyber forces will be ready to "operate alongside…air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Forces" (DOD United States, 2018).

In summary, the strategy is for the DOD to disrupt threats before the threat reaches U.S. networks and systems (Vergun, 2021).

However, the NDAA has provided the legal authority to shift toward a more offensive method. *Offensive cybersecurity* means "planting cyber 'weapons' deep within adversaries' networks" (Freiburger, 2019). According to various reports, the U.S. government under the Trump administration (2016–2020) has more aggressively deployed cyber tools against its enemies. *The New York Times* reported that U.S. officials confirmed placing American computer code inside Russia's electric power grid and other targets, an action "directed at Moscow's disinformation and hacking units around the 2018 midterm elections" in the United States (Sanger & Perlroth, 2019).

During the COVID-19 pandemic, there has been a significant growth in terms of the number of ransomware attacks against health facilities, which demonstrates the ways in which the growing digitalization trend has also expanded the threats and dangers of cybercrimes to various sectors (Collier, 2020).

While there remain challenges that need to be addressed, the U.S. government has tried to respond to the above-mentioned issues by investing resources to fight cybersecurity threats. Under the Trump administration's National Security Strategy, there had been a more vivid recognition that the United States is already operating within a multipolar environment, which takes into account the rise of great powers, such as China (as demonstrated in the two countries' agreements on cyberattacks). As such, this will potentially inform the policies and strategies of the United States in cyberspace. Given the emerging threats confronting the country, cybersecurity will continue to occupy a more prominent space on the U.S. national security agenda.

Key Takeaways

While the U.S. approach has many aspects worth emulating, there is still a lot of work to do in continuously developing technologies that are reflective of the new opportunities and threats within the cyber environment. Given that the United States is at the forefront of information security in terms of offensive and defensive capabilities, the Philippines can capitalize on some of the best practices from United States' cybersecurity policies and frameworks, which are hinged on an open ecosystem driven by cooperation among institutions and common standards.

One of the approaches that has worked for the United States places importance on public-private partnerships in promoting cybersecurity. The Philippine government can emulate this approach by looking at critical infrastructure in terms of information security and business continuity. The Philippines should also attempt to uphold minimum information security standards in the same level as those in FISMA, NIST SP 800-53, and the NIST cybersecurity framework. This means informational security standards should be used as a key baseline for cyber defense.

In promoting a cybersecurity program through several mechanisms, it is also important to bring into the picture the role of centralized authorities like the Certified Information Systems Auditor. There should be more efforts and resources from the Philippine government and private sector to invest in cybersecurity-related research and educational programs. In addition, the Philippines should recognize the need to properly adopt and develop its CERT. At the very least, the country should have a centralized coordinating body to get a comprehensive view of the cyber threat landscape. Given the country's vulnerability to cyberterrorism, the Philippine government cannot and should not do it alone. As recognized by the U.S. government, information security issues cannot be addressed by a single country. In a globalized and interconnected world, an attack on one can affect many others. Cybersecurity is a global issue that requires multilateral cooperation among different countries and international organizations.

Indonesia

Indonesia's digital transformation accelerated upon the completion of its USD 1.5-billion Palapa Ring project. The Palapa fiber optic network stretched 35,000 km over land and sea and provided 4G-capable Internet infrastructure (Medina, 2020). It boosted Internet connectivity to support the country's urbanization and digitalization program called 100 Smart Cities by 2045 Movement that was launched in 2017 (Samosir, 2020). Thus, it was no surprise that Indonesia saw a rise in online consumers since the start of the pandemic, with its Internet economy reaching USD 70 billion in 2021 and is expected to double to USD 146 billion by 2025 (Google et al., 2021).

Data protection and cybersecurity challenges in Indonesia have recently taken the spotlight. A surge in the number of cyber threats and attacks was recorded by the National Cyber and Crypto Agency, or the Badan Siber dan Sandi Negara (BSSN), Indonesia's cyber intelligence and cybersecurity agency. As of December 2021, BSSN reported 1.4 billion cyberattacks affecting government agencies and corporations, almost triple the 495 million traffic anomalies recorded in 2020 (Siregar, 2021). Recent cases of cyberattacks include the following:

- September 2021: Indonesian intelligence agency Badan Intelijen Negara and 10 government ministries were allegedly hacked by a Chinese group, Mustang Panda, but this was later denied by the Indonesian government (The Associated Press, 2021).

- August 2021: Indonesia’s COVID-19 test-and-trace mobile app, Electronic Health Alert Card (eHAC), exposed information from over 1.3 million of eHAC users to an open server (vpnMentor, n.d.). This, however, resulted when eHAC developers failed to put adequate data protection protocols in place (Chandra, 2021).
- July 2021: Cybercrime monitoring firm Hudson Rock reported that multiple computers belonging to the employees of Indonesia’s Bank Rakyat Indonesia (BRI) and its insurance arm BRI Life have been compromised, revealing sensitive data from around 2 million clients and 463,000 documents (Afifa, 2021).
- May 2021: Personal information of 279 million Indonesians was allegedly leaked and freely traded online in small samples at the database sharing forum Raidforum and were later on sold for 0.15 bitcoins (USD 6,130) for a larger set of the database (*Jakarta Globe*, 2021).

Indonesia’s cybersecurity threat landscape reflects that of other Association of Southeast Asian Nations (ASEAN) countries where businesses, public institutions, and critical infrastructure (e.g., telecommunications, energy, finance) are the constant targets of cyberattacks. The next section discusses the existing policies and mechanisms within Indonesia that protect against cyber threats.

Governance and Legal Structure

Indonesia before BSSN

Indonesia’s cybersecurity initiative began with the nongovernment organization Indonesia Computer Emergency Response Team (ID-CERT), established in 1998, which coordinates security incident handling, raises awareness on security issues, collects data, and researches security incidents (Rahardjo, 2017). Official government initiative only began in 2007 under the Ministry of Communications and Informatics (MOCI), which regulates the use of Internet-protocol-based telecommunication network and established the Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII) (Rizal & Yani, 2016). The ID-SIRTII is the national computer security incident response team of Indonesia tasked to communicate with various stakeholders related to Internet security (Asia Pacific Computer Emergency Response Team [APCERT], 2019). It detects and cautions stakeholders when any network disruptions take place (Rizal & Yani, 2016, pp. 69–70).

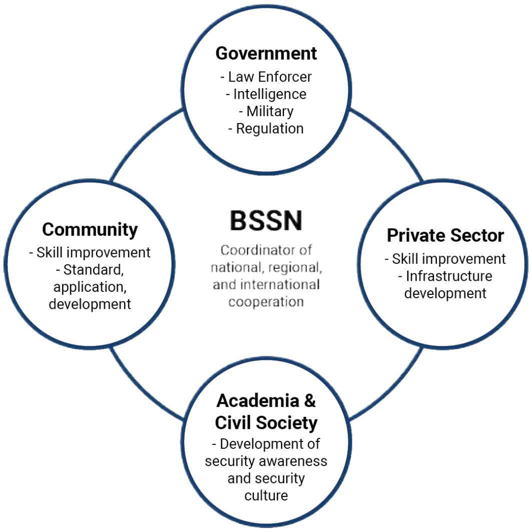
In conjunction with these efforts, there are a number of regulations and laws that support or mention the importance of cybersecurity.[9] According to Anjani (2021), two are of critical importance: (1) the Electronic Information and Transactions (EIT) Law No. 11/2008 and its revised version Law No. 19/2016; and the (2) Ministry of Defense (MOD) Regulation No. 82/2014. The EIT law covers cyber activities that are considered illegal (i.e., illegal distribution of content, breach of data protection, unauthorized access to computer systems to retrieve information, and illegal wiretapping) and accords overall legal protection for the contents of electronic systems and transactions (p. 4). MOD Regulation No. 82/2014 defines cybersecurity: “National cybersecurity comprises all efforts to secure the information and the supporting infrastructure at the national level from cyberattacks” (p. 4). It also covers within its mandate critical infrastructure (e.g., finance and transport). These two laws employ Indonesia's two-pronged regulatory approach to address its data privacy and cybersecurity issues: the EIT law covering nonmilitary cyber threats[10] and the MOD as a regulatory agency guarding national security and military-related cyber defense.

Other special laws on data privacy protection in specific regulatory areas include the Law on Health No. 36/2009, which deals with regulating activities related to storing patient medical records, and the Law on Banking No. 7/1992 as amended by Law No. 10/1998, covering the processing of personal and financial data by banks.

Mulyadi and Rahayu (2018) note that Indonesia's policy and regulation lack the synergy and coordination provided by a national cybersecurity strategy and a dedicated cybersecurity organization/department. More specifically, they point out that this structure and governance (1) only regulates information security and not the broad categories of cybersecurity;[11] (2) lack private sector engagement and joint strategizing for the protection of industries;[12] (3) and does not have an educational curriculum that discusses cybersecurity extensively (pp. 2–3). This fragmented legal and governance system continues to pose a great national risk to Indonesia, as it exploits the weaknesses and vulnerabilities of individual organizations and their people.

Establishing BSSN and the Cybersecurity Bill

Figure 2. BSSN Synergizes the Elements of National Security


Government
- Law Enforcer
- Intelligence
- Military
- Regulation
Community
- Skill improvement
- Standard, application, development
BSSN
Coordinator of national, regional, and international cooperation
Private Sector
- Skill improvement
- Infrastructure development
Academia & Civil Society
- Development of security awareness and security culture

Note. From "Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN)," by Mulyadi and D. Rahayu, in *6th International Conference on Cyber and IT Service Management (CITSM)* (p. 4), 2018, IEEE (https://doi.org/10.1109/CITSM.2018.8674265). Copyright 2018 by IEEE.

To address concerns over a national response to cybersecurity issues, the Indonesian government established the BSSN in 2017 through Presidential Regulation No. 53. The BSSN was formed through the combination of the National Crypto Agency (Lemsaneg),[13] the functions of the MOCI Information Security Director General, and the ID-SRTII.[14] Broadly, it has three duties (Mulyadi & Rahayu, 2018, p. 3):

1. Establish, implement, monitor, and evaluate the technical policy of national cybersecurity
2. Coordinate the role of cybersecurity with other organizations
3. Conduct national, regional, and international cooperation in the field of cybersecurity

As Figure 2 shows, the BSSN acts as a regulator for government organizations (e.g., Ministry of Justice and Human Rights, police, national intelligence agencies) and closely coordinates with the community, private sector, academe, and civil society to improve standards, skills, and overall education and awareness regarding cybersecurity issues.

Saputra et al. (2019, p. 113) point out that BSSN still has limited capacity over leading cybersecurity because its mandate (especially on critical infrastructure) is only based on presidential regulations. Saputra et al. noted that these rules do not legally bind other parties (mainly, the private sector) toward the guidelines set by the BSSN. Furthermore, the existing legal and regulatory environment still do not cover a range of issues. For instance, establishing the difference between cyber defense attacks (which is the mandate of the defense ministry) and cybercrimes (which is the mandate of the police) remains an issue within government agencies (Chairil, 2019).

Despite the efforts of the BSSN to present cybersecurity regulations, Indonesia continues to experience increasing costs of cyberattacks. In 2018, BSSN reported 232 million cyberattacks, with cybercrime causing USD 33.7 billion in economic damage, prompting Indonesian lawmakers to discuss a comprehensive solution—a cybersecurity bill (Sihaloho & Yasmin, 2019). Thus, in 2019, the Cybersecurity and Cyber Resilience Bill (*Rancangan Undang-Undang Keamanan dan Ketahanan Siber*) was proposed in Indonesia's House of Representatives. The bill clarified the implementation of cybersecurity, the role BSSN plays in these plans, and other critical guidelines for governance, law enforcement, and diplomacy.[15] It mandates BSSN to develop a national cybersecurity strategy and, more crucially, addresses the gaps in the EIT law, stipulating protections for information security and network infrastructure (Anjani, 2021).

However, the proposal repeated many of the uncoordinated and fragmented efforts that exist within Indonesia's governance and legal structure. For instance, Article 38 of the proposal suggests that BSSN "filter electronic content and applications containing harmful content to protect the safety of the community when using electronic applications," but these functions are already present under the MOCI (Anjani, 2021, p. 5). Anjani attributes these policy mishaps to the closed policymaking process in making the cybersecurity bill. From the bill not being available online to the MOCI not involved in writing the proposal, Anjani said the noticeable lack of consultation and deliberation saw the cybersecurity bill neglect existing cybersecurity paradigms as evidenced by duplicating regulations.[16] The cybersecurity bill proposes to grant a "super agency" status to its implementing body, superseding law enforcement institutions, and the potentially dangerous censorship power granted to this body to determine what constitutes as "harmful" content (Chairil, 2019). As the bill lacked input from other government stakeholders, Indonesia's House of Representatives was not able to pass the proposal into law. It will continue to be deliberated in 2022.

Recently, there were efforts from the executive branch to strengthen the BSSN. In April 2021, President Joko Widodo signed Presidential Regulation No. 28 of 2021 on the BSSN "based on the need to organize the agency in the context of realizing national cybersecurity, protection, and sovereignty, as well as increasing the national economic growth." The Presidential Regulation said "a more effective and efficient BSSN organization is needed" to achieve its cybersecurity goals, which entails improving the structure, duties and functions, organization, working procedure, and funding of BSSN" (Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation, 2021).

Major Cases of Indonesian Cyberattacks

In 2017, the WannaCry malware spread rapidly across networks globally, infecting Windows computers to encrypt hard drives and making it impossible for users to access their data until they pay ransom for decryption (Fruhlinger, 2018). Two of Indonesia's major hospitals were targets of this ransomware attack, locking up their IT systems containing patient records and billings (Reuters, 2017). Following the attacks, the MOCI disseminated instructions on system updates and Internet connections, and the National Police's cybercrime unit coordinated with international law enforcement agencies (*The Jakarta Post*, 2017). Hospitals had to reinstall their systems from backup computers and servers, causing operational delays (Reuters, 2017).

More recently in the 2019 Indonesian general elections, infiltration claims of Chinese and Russian "ghost voters" loomed—claims that its election commission (Komisi Pemilihan Umum or KPU) said were most likely homegrown rather than foreign (Lamb, 2019). An IT infrastructure consultant for the KPU says that hacking attempts on its voter database were normal but had a zero success rate as the agency was able to remove questionable within its election list (Lamb, 2019). However, in 2020, a breach of election data saw 2.3 million voters' private data (i.e., home addresses, national identification numbers) released in a hacker website, with threats of releasing 200 million more (Widianto & Potkin, 2020). Many experts have called for a comprehensive forensic audit of the breach, with some calling for more action from the BSSN as it has "yet to function optimally" to prevent such attacks from happening (Pinandita, 2020).

Key Takeaways

Like other ASEAN countries, Indonesia's current cybersecurity policy environment is still developing:

1. Indonesia has the foundations of a robust cybersecurity framework. Its two-pronged legal structure covers elements for civilian protection as well as national protection. Despite its weaknesses, government regulations remain a key driver for implementing cybersecurity measures.[17]

2. While Indonesia's cybersecurity framework spans many laws, regulations, and government institutions, having a coordinated and cohesive response to make it effective remains a challenge. In comparison other countries with well-developed cybersecurity frameworks that employ a "whole-of-government" approach, Indonesia is still in the process of consolidating its laws, regulations, (through the Cybersecurity Bill) and organizations (through the BSSN).

3. The current cybersecurity bill was crafted through a closed policy process, which critics say makes it unresponsive to cybersecurity issues faced by different Indonesian organizations. Given that the threats and attacks target a broad range of institutions and individuals, it is critical to acquire their buy-in for the proposal as its successful implementation relies on their willingness to follow new guidelines.

Endnotes

1 “Cybersecurity framework” refers to the system of concepts, rules, and practices dictating the direction of policies and regulations, including the implementation of legal, technical, and political tools to align with the overall goals of a country or other entity (National Institute of Standards and Technology, 2018b).

2 List was taken from Commonwealth of Australia (2009, p. 24) with some updates.

3 The Five Eyes alliance involves secretive intelligence gathering and sharing operations between the security agencies of the United States, the United Kingdom, Australia, Canada, and New Zealand. See Privacy International (n.d.).

4 Exemptions from Israeli military service are granted based on various grounds, including exemptions on religious or conscientious grounds, among others. See Pex (n.d.).

5 Other international agreements are with Cyprus, Czech Republic, Ethiopia, Greece, Honduras, Kenya, Rwanda, South Sudan, Tanzania, Uganda, and Zambia.

6 In February and March 2014, Russia invaded Crimea and annexed it from Ukraine. The move was made in response to the ousting of Ukrainian President Viktor Yanukovych through popular demonstrations. The Russian government supported Yanukovych for his refusal to sign a political and free-trade association agreement that would align Ukraine closer with the European Union.

7 For the latest version of the NIST SP 800-53, see Joint Task Force (2020).

8 “Authentication” refers to the process of verifying the identity of a user, process, or device before providing access to a secured network or system (National Institute of Standards and Technology, 2006).

9 To see a comprehensive list of laws, presidential regulations, and MOCI guidelines that support or relate to cybersecurity, see Rizal and Yani (2016, pp. 68–70).

10 Other privacy breaches are covered by other laws, including Indonesia’s Criminal Code, which penalizes confidentiality breaches that may expose personal data for malicious use, and the Telecommunications Act of 1999, which requires telecommunications service providers to uphold confidentiality of information from their customers.

11 For instance, the EIT law only covers illegal activities done on electronic systems and transactions but does not adequately address the information and network infrastructure targeted and impacted by these attacks, nor does it stipulate requirements for cybersecurity experts within human resources of organizations (Anjani, 2021).

12 As Rizal and Yani (2016) point out, the implementation of cyber defense in Indonesia is still sectoral and optional, reliant on the interests and capacities of various private, nongovernment, and public organizations. For instance, the MOCI’s Information Security Index (Indeks Keamanan Informasi or Indeks KAMI), which evaluates the strength of government agencies’ cybersecurity measures, is not compulsory for all government entities (Rahardjo, 2017).

13 The National Ciper/Crypto Agency is a specialized unit dealing with the security of ICT resources, especially with regard to signals intelligence or cryptography (Rizal & Yani, 2016, p. 72).

14 Presidential Regulation No. 53 of 2017 merged and moved the ID-SIRTII to BSSN’s National Cyber Security Operation Center (APCERT, 2019, p. 142).

15 A recent example of cyber diplomacy relates to Indonesia’s renewal of its 2018 bilateral agreement with Australia. The agreement fosters information sharing, capacity building, and cooperation between the two countries in addressing cybersecurity and cybercrime issues (Australian Government, 2021).

16 For instance, Anjani (2021) points to the proposed cybersecurity bill’s Article 17 (which requires businesses to get BSSN certifications for cybersecurity products), Article 19 (which requires human cybersecurity

resources to meet BSSN standards), and Article 21 (which requires cybersecurity personnel to acquire certifications from other accredited BSSN organizations) not being different from existing ITE law regulations or MOCI mandates, creating a duplication of requirements.

17 Rahardjo (2017) uses the example of Indonesian bank regulations that require financial institutions to periodically perform security audits of their systems and the vendors that provide services to them.

PART 2:

Philippine Cybersecurity Issues and Challenges

Digitalization in the Philippines is constrained by barriers, such as outdated policy and regulation, poor access to high-speed Internet connection, and lack of support infrastructure (e.g., logistics, digital payment). But like many developing countries, mobility restrictions and extended lockdowns due to COVID-19 have pushed millions of Filipinos to adapt to a digital existence. The Bangko Sentral ng Pilipinas reports that over 20% of transactions were electronic in 2020. Surveys show significant growth in online shopping and use of cashless payment among Filipinos by almost 60% in the same year. GCash, a mobile wallet company, reported an increase of users by 130% between January 2020 and June 2021, with peak logins of 15 million per day in the second quarter of 2021.

However, with more digital activities come higher cybersecurity risks. Kaspersky, a global cybersecurity firm, estimates that 37% of online users in the Philippines had experienced some form of cyberattack and an increase by almost 60% of web threats detected in the country in 2020. As more individuals and organizations go online, malicious actors have more opportunities to exploit vulnerabilities, thus increasing the risks for individuals, businesses, and government.

Part 2 is an attempt at capturing the state of cybersecurity in the Philippines by looking at cybersecurity issues and practices in key sectors. It concludes with a set of key findings and recommendations on how the country can improve its cybersecurity posture.

Chapter 4 provides a review of the major cybersecurity issues and challenges encountered in e-government, e-commerce, online banking, and remote work; in key sectors, such as health, education, energy, water, transportation, and telecommunications and Internet; in important events, such as the automated elections; and flagship programs, such as the National ID.

Finally, Chapter 5 details the report's key findings based on industry experience and consultations with a range of stakeholders, and concludes with recommendations on how to improve the Philippines' cybersecurity posture.

4 | State of Philippine Cybersecurity: Critical Infrastructure and Key Sectors

> *While it seems that developed countries are more prone to cyberattacks, developing countries such as the Philippines may also be dragged into the cyber warfare between great powers or into geopolitical disputes against neighboring countries.*

Cybersecurity encompasses the protection of both publicly and privately owned or maintained resources. Key sectors, such as energy, water, and telecommunications, which are considered critical infrastructure, necessitate the implementation of more stringent cybersecurity measures.

Critical Infrastructure

"Critical infrastructure" or CI refers to assets, systems, and networks, whether physical or virtual, that are considered so vital that their destruction or disruption would have a debilitating impact on national security, health and safety, or economic well-being of citizens, or any combination thereof.

This definition can differ from one country to another, given that what is considered critical or essential for one nation may not be the same for another.[1] The classification of critical infrastructure can also change over time. However, a common feature across various jurisdictions is that these infrastructures are vital to the continuous delivery of services that are essential to everyday life in a country.

In the Philippines, critical infrastructure is defined in several government issuances and documents.

In 2001, President Gloria Macapagal Arroyo (2001–2010) issued Memorandum Order No. 37, which defined critical infrastructure by way of enumeration: "power plants, power transmissions and distribution facilities, oil and gas depots, key public work structures, vital communications installations, public and private buildings and other facilities in the center of commerce and industry."

Possibly the earliest definition of critical infrastructure was coined by the Department of Energy in 2004:

> "[Critical infrastructures] are…key infrastructures not only for economic growth and development but also as societal instruments for the conduct of everyday activities. Hence, any threat posed against these infrastructures would be threats to national security."

Critical infrastructure was also defined in the Cybercrime Prevention Act of 2012, but the focus was on computer systems and networks:

> "[T]he computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data that are so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters" (Sec. 3 (j)).

The Philippines' National Cyber Security Plan 2022, issued in May 2017, listed as one of its primary goals "assuring the continuous operation of the nation's critical infostructure (information infrastructure)," or CII.[2] According to the plan, "the functions and services of critical infostructure and those of the governmental bodies are vital to the country's socioeconomic activities," such that "any interruption of these functions and services can cause direct and significant consequences to people's safety and security." The cybersecurity plan expanded the list of CI identified in Memorandum Order No. 37, s. 2001 and adopted the list of CII from the Cybersecurity Strategy of Singapore (Department of Information and Communications Technology, 2017a).

In September 2017, the Department of Information and Communications Technology issued a department order on the protection of CII and adopted the definition of CI found in the Cybercrime Prevention Act (2012). The order identifies the sectors *initially* classified as CIIs as follows:

1. Government
2. Transportation (land, sea, air)
3. Energy
4. Water
5. Health
6. Emergency services and disaster response
7. Banking and finance
8. Telecommunications
9. Media
10. Business process outsourcing

Due to its importance, critical infrastructure has increasingly become a target of cyber threats over the last decade. Cyberattacks are now used to disrupt the operation of infrastructure, such as water systems, gas pipelines, and power grids, with dire consequences in the physical world. Malicious actors range from individual hackers wanting to cash in on the chaos, to government-sponsored groups fueling nation-state rivalries. The wider the devastation, the more complex the cyberattack.

Criteria for defining critical infrastructure

Recognizing the severity and magnitude of the devastation effected by cyberattacks to the economy, peace and order, and overall well-being of citizens, it is important for countries to identify critical infrastructure that must be secured and protected.

There are different ways to classify a sector as critical infrastructure. The EU looks at critical infrastructure from two sets of criteria: cross-cutting and sectoral. The *cross-cutting criteria* comprise (1) casualties, (2) economic effects, and (3) public effects. Its thresholds are based on the severity of the impact of the disruption or destruction of a particular infrastructure. The *sectoral criteria* take into account the characteristics of individual European CI sectors (European Union, 2008). Meanwhile, Malaysia considers the impact of CI disruption not only on the national economy, security, government, and public health and safety, but also on *national image*.

These nuances also apply to classifying critical information infrastructure. Singapore, for example, defines a CII as a computer or computer system *located wholly or partly in Singapore*. This means Singapore's regulation on CII may cover ICTs physically located outside the city-state.

Based on the authors' analysis, the following set of criteria is recommended for identifying critical infrastructure in the Philippines, based on the assessment of potential disruption to operations or destruction of systems and assets:

1. *Size* — the size or geographical scope of operation in key sectors
2. *Casualties* — the potential number of fatalities or injuries
3. *Economic effects* — the significance of economic loss and/or degradation of products or services, including potential environmental effects
4. *Public effects* — the impact on public confidence, physical suffering, and disruption of daily life, including the loss of essential services

Below is a list of critical infrastructure sectors identified by select countries based on their own set of criteria, as of February 28, 2022.

Table 2. Critical Infrastructure Sectors in Select Countries

Critical infrastructure	United States[3]	European Union[4]	Australia[5]	Singapore[6]	Malaysia[7]	Philippines
Government[8]	●	●	●	●	●	●
Energy[9]	●	●	●	●	●	●
Water[10]	●	●	●	●	●	●
Banking and Finance	●	●	●	●	●	●
Communications[11]	●	●	●	●	●	●
Health[12]	●	●	●	●	●	●
Transportation[13]	●	●	●	●	●	●
Emergency services	●	●		●	●	●
Food[14]	●	●	●		●	
Security[15]	●		●	●	●	
Media				●		●
Business process outsourcing						●
Chemical sector[16]	●	●				
Commercial facilities	●					
Critical manufacturing	●					
Dams[17]	●					
Data storage or processing			●			
Higher education and research			●			
Nuclear reactors, materials, and waste	●	●				
Space and research		●	●			

The seven sectors commonly identified as critical infrastructure by the United States, the European Union, Australia, Singapore, Malaysia, and the Philippines are as follows: government services, energy, water, banking and finance, communications, health, and transportation. Since what is considered vital to a country's functioning may change over time, the list of critical infrastructure is not, and *should not be*, static.

CI institutions are responsible for the protection of critical infrastructure against threats and attacks. CI institutions are entities, whether public or private, that own, operate, control, and/or maintain critical infrastructure. Considering the size, casualties, economic effects, and public effects criteria, CI institutions in the Philippines may refer to those whose operation is nationwide in scope and/or covers metropolitan centers,[18] including Metro Manila, Metro Cebu, Metro Davao, Metro Cagayan de Oro (by 2025), and other metropolitan centers to be identified in the future.

The first step to keeping critical infrastructure safe and secure is to require CI institutions to comply with minimum information security standards. The government agency and/or regulator must be responsible for issuing the policy, enforcing, and monitoring compliance to such standards within their sector of jurisdiction. Hence, CI institutions must strive to develop a deep understanding of the cybersecurity challenges faced by their respective sectors, access the necessary resources, and build their capacity (technology, people, and process) to prevent and respond to cyber incidents.

Below are some examples of CI institutions in the Philippines, including the government agency and/or regulator responsible for promoting and enforcing cybersecurity standards in select sectors. Given the evolving global and local environments, as well as the changing realities of industries, a continuous discussion about the criteria for determining critical infrastructure in each sector is strongly encouraged.

Table 3. Examples of CI Institutions in Select Sectors in the Philippines

Sector	Government Agency and Regulator	Owner/Operator
Energy	Department of Energy National Transmission Corporation Energy Regulatory Commission	National Grid Corporation of the Philippines, Manila Electric Company, and power distribution companies that operate in metropolitan centers
Water	Metropolitan Waterworks and Sewerage System National Water Resources Board	Manila Water Company, Maynilad Water Services, and water supply companies that operate in metropolitan centers
Banking and Finance	Department of Finance Bangko Sentral ng Pilipinas	BDO Unibank, Metropolitan Bank & Trust Co., Bank of the Philippine Islands, and other banks with nationwide coverage or operations in metropolitan centers

Table 3. Continued

Transportation	Department of Transportation Civil Aviation Authority of the Philippines	Ninoy Aquino International Airport Philippine Airlines, Cebu Pacific, other aircraft operators, and cargo operators in the aviation industry that operate nationwide or in metropolitan centers
Telecommunications	National Telecommunications Commission	Smart Communications, Globe Telecom, Dito Telecommunity, Converge ICT, and other telcos with nationwide coverage or operations in metropolitan centers
Media	National Telecommunications Commission (radio spectrum)	ABS-CBN, GMA, and other TV and radio stations with nationwide coverage or operations in metropolitan centers

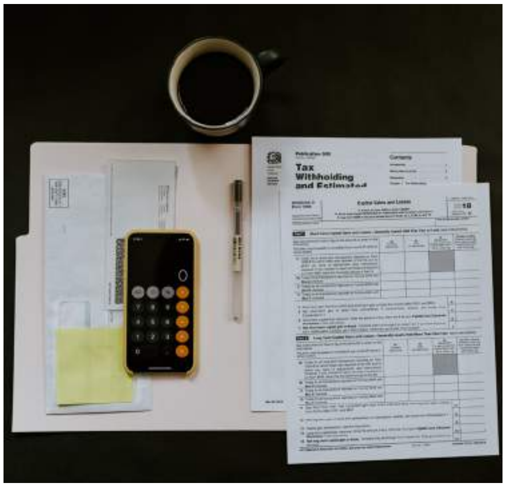
In the absence of a law on cybersecurity, the impact of the Data Privacy Act of 2012 (DPA), or Republic Act 10173, in compelling many enterprises to adopt cybersecurity measures cannot be minimized. At present, compliance with the data security provisions of the DPA already compels any enterprise, whether public or private, that controls the processing of personally identifying information, to adopt "reasonable and appropriate organization, physical, and technical measures intended for the protection of personal information[19] against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing" (DPA, 2012, Sec. 20). The National Privacy Commission (NPC) is likewise empowered to prescribe safeguards that these personal information controllers should implement to protect their computer networks against accidental, unlawful, or unauthorized usage or interference, as well as security policies with respect to the processing of personal information. The compliance requirements of the DPA, therefore, entail the adoption of cybersecurity measures by enterprises that process personal information. Considering the broad definition of "processing" under the DPA as to encompass any meaningful engagement with personal information,[20] the scope of enterprises that are compelled to adopt comprehensive data security policies to comply with the DPA is necessarily wide.

Nonetheless, even without any compulsion from the state, it remains best practice for private enterprises to consider and adopt cybersecurity measures upon their own initiative. After all, the risks to enterprises that cybersecurity failures pose extend to compromising consumer confidence and financial losses, not just the threat of state sanction arising from the failure.

The next section is a review of the state of cybersecurity in key sectors, existing policy frameworks that impact cybersecurity, and recommendations on ways to mitigate risks and develop cyber resilience.

Electronic Government

President Rodrigo Duterte has declared that he wanted every government transaction to be done online (Lamiel, 2017). This echoes the mission of the National Government Portal, GOV.PH, to serve as "a single window uniting all web-based government content to maximize efficiency and provide rapid, high-quality services to citizens" (GOV.PH, n.d.).



The president's statement has gained new relevance during the pandemic, with lockdown restrictions severely limiting people's mobility, even as the need for government services remains. Many government agencies were impelled to move some of their processes and services online to minimize or eliminate face-to-face engagements in light of health and safety considerations. The shift was facilitated by an issuance by the Civil Service Commission, which guided government agencies on work-from-home arrangements, skeletal workforce, and condensed or staggered work times with the aim of providing additional opportunities to decongest the workplace for social distancing.[21]

The Department of Trade and Industry (DTI) used its website to promote COVID-19-related resources, DTI issuances, news, advisories, and information kits. With the president prohibiting face-to-face classes, the Department of Education (DepEd) moved enrolment to email, social media, or designated kiosks in government offices. DepEd's self-learning modules now include both blended and online learning.

Congress also moved its proceedings online. The Senate allowed plenary sessions and committee hearings through teleconferencing (Senate of the Philippines, 2020). Voting was done via Webex's polling feature to accommodate senators who were not physically present at the session hall. Similarly, the House of Representatives conducted hybrid plenary sessions and hearings, where voting by electronic means was allowed.

The Supreme Court likewise took the unprecedented step of allowing the online submission of filings, application for bail, and issuance of orders by electronic means or email. It designated first- and second-level courts nationwide that may conduct hearings through video conferencing and allowed the raffling of cases through video conferencing.[22]

Cybercriminals have likewise made the shift, imposing themselves in schemes that involve the delivery of government services.

During the pandemic, scammers operated through SMS and Facebook by swindling money from government cash aid beneficiaries. Fake Facebook groups and representatives, claiming to be from the Department of Social Welfare and Development, have tricked beneficiaries into giving their personal identification numbers (PIN), one-time PIN, or card verification code (Macapagal, 2020).

Still, the shift of public services to an online environment is helping validate the thesis that e-government[23] is viable in the Philippines. Several laws and policies enacted prior to the COVID-19 pandemic have started to prepare the Philippines for this eventuality, but it remains to be seen whether the transition would further accelerate even as the pandemic recedes.

Policy Frameworks Enabling Electronic Government or E-Government

National ICT Frameworks in Government

The attempt to harness information and communications technology (ICT) in government started in 1997, with the crafting of the National Information Technology Plan for the 21st Century, followed by the Government Information Systems Plan in 2000, the Philippine Strategic ICT Roadmap (2006–2011), and the Philippine Digital Strategy (2011–2016). The E-Government Master Plan (2013–2016) envisions "a digitally empowered and integrated government that provides responsive and transparent online citizen-centered services for a globally competitive Filipino nation." The current framework is the E-Government Master Plan 2.0 (2016–2022).

Electronic Commerce Act

The Philippine government has long laid the legal framework for moving public sector processes online. Republic Act (RA) No. 8782 or the Electronic Commerce Act (e-Commerce Act) of 2000 aims to promote government-to-citizen (G2C), government-to-business (G2B), and government-to-government (G2G) transactions by electronic means. The law provides for the legal recognition of electronic data messages, documents, and signatures (e-Commerce Act, 2000, Sec. 6–8). This means all commercial and noncommercial documents generated, signed, transmitted, and received electronically have the same legal effect and validity as traditional paper-based documents and can be accomplished remotely.

The e-Commerce Act mandates all government agencies and instrumentalities, government-owned and controlled corporations, state universities and colleges, and local government units (LGUs) to enable electronic transactions that may be initiated and paid for (where appropriate) digitally, and through which the agency may issue permits, licenses, or certificates of registration or approval. It also mandates the installation of an electronic online network, called RPWEB, which shall be the government information infrastructure to enable G2C, G2B, and G2G electronic transactions. RPWEB's roots can be traced to a Ramos administration (1992–1998) order to provide a virtual interconnection of all government offices and schools (Administrative Order 332, s. 1997).

The DTI, the Department of Budget and Management, and the Bangko Sentral ng Pilipinas (BSP) are the key implementing agencies of the e-Commerce Act of 2000 (Sec. 34). The Department of Transportation and Communication (since separated into the Department of Information and Communications Technology and the Department of Transportation [DOTr]), National Telecommunications Commission (NTC), and the former National Computer Center[24] are tasked to promote and implement a policy and regulatory environment to facilitate the development of the government information infrastructure.

The Supreme Court has also promulgated the Rules on Electronic Evidence and subsequently rendered decisions on the admissibility of electronic data messages and electronic documents as evidence.[25] Today, not only is digital evidence admissible, but digital versions of traditionally physical documents, such as contracts and agreements, can also be used in court. This is significant for e-government processes because when disputes arise in government transactions, electronic documents, such as digitally signed contracts, may be presented in court as evidence.

Government Web Presence

Soon after the enactment of the e-Commerce Act, government agencies started building their respective websites to provide information to the public. RPWEB started the efforts to establish e-government. The latest iteration is the Integrated Government Philippines (iGOV.ph) program. Launched in 2012, iGOV.ph seeks to achieve a higher level of e-governance or the application of ICT to rationalize government operations and improve the delivery of goods and services to the people (iGov Philippines, n.d.). The iGOV.ph program sets certain minimum standards, which aim to harmonize and ensure the interoperability of different government agency websites.

Government agencies have gradually offered dynamic websites that enable citizens to transact with government agencies electronically. Below are some examples:

- The DTI's Business Name Registration System allows a citizen to apply for business name registration, pay electronically, and receive the certificate of registration via email (DTI, n.d.).
- The Commission on Audit's (COA) Citizens' Desk Report System allows for the filing of queries, complaints, requests, and reports on allegations of fraud, waste, or mismanagement of funds (COA, n.d.).
- The Bureau of Customs' Customer Care Portal allows citizens to track parcels and *balikbayan* boxes or track shipping documents (Bureau of Customs, 2021).

The Philippine National Public Key Infrastructure and Digital Signatures

A digital signature is a type of electronic signature that allows independent verification of the identity of a signer to an electronic document. A public key infrastructure (PKI) authenticates users and devices, allowing "one or more trusted parties [to] digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device. The key can then be used as an identity for the user in digital networks" (SSH.com, 2021).

In 2009, President Gloria Macapagal-Arroyo issued Executive Order No. 810, which institutionalized the certification scheme for digital signatures and directed the application of digital signatures in e-government services. In response, the Department of Information and Communications Technology (DICT) developed and built the Philippine National PKI (PNPKI).

At the core of the PKI are the digital certificates, issued to natural persons, software applications, or devices, which are digitally signed by a trusted party called a certificate authority—in this case, the DICT. These certificates allow the PKI to attest to the identity of documents or data transmitted online. The DICT offers the PNPKI as a service available to all government agencies, personnel, and private citizens. Electronic devices and software applications may also be enrolled in the PNPKI.[26]

Ease of Doing Business

RA 11032 or the Ease of Doing Business and Efficient Government Service Delivery Act of 2018 (EODB Law) amended RA 9485, or the Anti-Red Tape Act of 2007. The EODB Law aims to increase efficiency in the delivery of government services by prescribing the number of days within which business-related transactions may be processed, depending on the complexity of the transactions and considering other factors, such as public health and safety, public morals, public policy, and highly technical applications.

Promoting a zero-contact policy, the EODB Law also seeks to eliminate red tape, avert graft and corrupt practices, and promote transparency through the establishment of a central business portal, which will receive business-related transactions, including applications for business licenses and permits issued by LGUs.[27] It also mandates the establishment of the Philippine Business Databank, which shall serve as a repository of all information about registered businesses nationwide to which all LGUs and national government agencies shall be connected. Both the central business portal and the Philippine Business Databank shall be developed, maintained, and operated by the DICT.

Status of Use of Electronic Documents and Electronic Signatures in Government Transactions

In the 20 years since the promulgation of the e-Commerce Act, paper-based and hand-signed documents remain the definitive versions of contracts, transactions, and reports in both the government and private sectors, even if these were initially prepared using electronic means. The difficulty in securing digital signatures and the dearth in government-accredited private certificate authorities account for some of the challenges to utilizing electronic documents as definitive when establishing contracts and transactions.

The COA issued Circular No. 2015-007 on October 22, 2015, prescribing the *Government Accounting Manual for Use of All National Government Agencies*, which provides for, among others, the use of electronic documents as evidence of collections, deposits, and disbursements (COA, 2015). The COA, however, has yet to issue rules on the acceptability of electronically signed electronic contracts between government agencies and private sector suppliers, a stumbling block to fully transitioning to e-government, as of writing.

National Cybersecurity Plan 2022

The **National Cybersecurity Plan (NCSP) 2022**, released by the DICT in 2017, aims to ensure the continuous operation of the Philippines' critical information infrastructure (including public and military networks); implement cyber resiliency measures to enhance the country's ability to respond to threats before, during, and after attacks; provide effective coordination with law enforcement agencies; and develop a cybersecurity educated society (DICT, 2017a).

As part of the Plan, the DICT's Cybersecurity Bureau is promoting the creation of computer emergency response teams (CERTs) in government agencies and business organizations and organizing the CERTs into government and industry sectors. This is complemented by cybersecurity awareness activities, including partnerships with the academe, such as the introduction of cybersecurity courses in private universities.

Cybersecurity Risks for Remote Government Work

As with other forms of remote work, the shift of government processes and services online carries certain risks and threats. The following are the most common risks to remote work, particularly for the public sector:

- *Bring Your Own Device (BYOD).* Government employees using personal devices to remotely connect to office systems are potential points of vulnerability. Because of the sudden shift to work-from-home arrangements brought about by the pandemic, IT departments may not have had the luxury of time to vet personal devices to ensure that security solutions are installed and properly configured for secure remote access to the organization's office system.
- *Connectivity.* In today's environment, users normally connect to office systems using virtual private networks (VPNs) to secure their traffic via the Internet. Users, however, may be unaware of or unfamiliar with the use of VPNs, and government information technology (IT) departments may not have implemented two-factor or multifactor authentication solutions to grant secure access to office systems.
- *Teleconferencing.* There has been a surge in the use of teleconferencing applications for virtual meetings and webinars among government institutions. Malicious actors have been known to infiltrate video conferencing applications, in particular Zoom, with applications such as zWarDial, an automated tool that looks for unprotected Zoom meetings (Peters, 2020). Once in a teleconference, an attacker can then engage in credential harvesting, phishing attacks, identity theft, frauds and scams, and other similar malicious behavior.

The transition to e-government is a constant challenge of adopting current technology and anticipating future ones. As we move toward more digital transformation in government, information security becomes more critical, and being able to protect information will be of primary importance. The following recommendations will help achieve information security in the adoption of e-government:

1. Government agencies must adopt and implement the minimum standards for interoperability and information security among government agency systems. Minimum interoperability provides the basis for creating an interoperable e-government ecosystem. With the promotion and use of application programming interfaces (APIs) and standards, growth can be achieved by capability sharing among the various government IT systems. Eventually, this allows the country to build an API economy. On the other hand, minimum information security standards provide the baseline for securing this information infrastructure.

2. Promote the use of electronic documents and electronic signatures for electronic transactions with the government. The digitalization of government processes has been a long, slow journey, but the pandemic pushed government agencies to digitize their frontline services. However, digital transformation of backend processes will require a lot more effort and political will to accomplish. If there were more systems and services already digitized, could the government have responded to the lockdowns more quickly and easily? This covers not only the transactions themselves but also the aspects of the documents and digital identity.

3. Consistent with Item 2, the COA should promulgate rules on the accounting and auditing of electronic transactions, specifically on the use and acceptability of electronically or digitally signed electronic contracts. Digital signing of electronic documents provides another layer of security, as it allows for independent verification of the signer's identity.

4. The DICT must secure international recognition of the PNPKI and ensure that government agency websites are secure with the proper Secure Sockets Layer (SSL) certificates.

    a. DICT's PNPKI offers opportunities for government agencies, business organizations, and individuals to better secure their networks, applications and systems, devices, and the digital identities of employees and individuals.
    b. Government and private sector entities may have their devices, applications, and systems enrolled in the DICT's PNPKI and have employees secure their individual digital certificates to secure documents and communications.
    c. Individual citizens must also be encouraged to secure their own digital certificates to enable them to digitally sign electronic documents and email communications.

5. For those managing security systems and electronic devices in the public sector, ensure that the software used is the latest version and that the latest patches are applied, and that all users share the responsibility of maintaining cybersecurity by
   a. promoting cybersecurity hygiene among users;
   b. conducting regular cybersecurity awareness among end users;
   c. performing regular security assessments; and
   d. building and practicing proper information security response and restoration practices.

Electronic Commerce

E-commerce has been defined by the World Trade Organization as the production, distribution, marketing, sale, or delivery of goods and services via electronic means, including Internet retail, digital media, online travel, ride-hailing, and digital financial services (DTI, 2021). The Philippine government has identified e-commerce as a driver of future growth (National Economic Development Authority [NEDA], 2020). The country's economy is consumption driven, and it seems that it will continue to be so postpandemic. A Google official noted in an interview that despite the economic contraction, e-commerce has grown 55% in 2020 (ABS-CBN News, 2020b). Indeed, Google's *e-Conomy SEA 2020* report notes that the country's e-commerce gross merchandise value grew to USD 7.5 billion in 2020 and is expected to reach USD 2 billion in 2025 (Google et al., 2020).

The mobility restrictions imposed in 2020 led to an increase in consumers going digital. Small and large businesses moved their stores online to continue reaching their customers. There was also a huge increase in mobile wallet registrations, as well as online and mobile banking transactions, as Filipinos transitioned to buying their needs online.

An increase in digital adoption also means an increase in cybersecurity risks. With the rapidly transforming digital economy, securing cyberspace must be a priority. In his 2020 State of the Nation Address, President Duterte stated that the government will prioritize safe online commerce in the new normal and committed to protect both the "physical and digital lives" of Filipinos (Duterte, 2020).

There are millions of Filipinos online, usually through smartphones, who avidly use social media; this wide base of social media users also makes it easy for online businesses to cross-post and use the platform to advertise their products that are in popular e-commerce marketplaces in the country, like Shopee and Lazada.

According to a 2021 report, 89% of the country's 74 million Internet users have searched online for a product or service to buy, and about 80% have made an actual purchase (Kemp, 2021). According to the same report, the top three consumer categories that saw growth in e-commerce spending in 2020 were food and personal care, furniture and appliances, and toys and hobbies.

The means of payment is also important to e-commerce. This interdependence between online shopping and the method of payment may have contributed to the accelerated adoption of mobile wallets and mobile and online banking, especially during the lockdown.

The Philippines has laws in place to protect individuals online, such as the e-Commerce Act, the Data Privacy Act, and the Cybercrime Prevention Act. More recently in 2020, the House of Representatives passed the proposed Internet Transactions Act on third reading, which aims to strengthen protection for consumers who purchase goods and services from online businesses (Cervantes, 2020b).

Cyber Threats

Cyber criminals are targeting both retailers and consumers. The International Criminal Police Organization (Interpol), in its 2021 Association of Southeast Asian Nations (ASEAN) cyber threat assessment report, identifies the top regional cyber threats: business email compromise (BEC), phishing, ransomware, e-commerce data interception, cyber scams, cryptojacking, and crimeware-as-a-service.

Ransomware, phishing, cyber scams, and BEC are persistent problems, but the scale of attacks has increased especially during the lockdown. Web skimming, a form of e-commerce data interception where bad actors steal personal and financial information from infected websites, has also increased. Security researchers have seen a variation of how this Magecart script is inserted to avoid detection. The Dutch security firm Sanguine Security has reported that close to two-thirds of its investigation found invisible web skimmers in databases, PHP code,[28] or a Linux system (Cimpanu, 2020d). On the other side of the globe, distributed-denial-of-service (DDoS) attacks targeting e-commerce have quadrupled in Europe, with these attacks often accompanied by ransom notes (Raywood, 2020).

E-commerce sites are prime targets for cybercriminals, particularly for customers' information and credit card data. With more businesses online and more customers shopping online, the interest is in harvesting customers' personal identifiable information and payment card details that retailer sites collect and store. The information is used to hijack personal accounts or to ransom or sell them on the dark web. Some of these attacks include brute force attacks, like what happened with Alibaba in 2016, denial-of-service (DoS) and DDoS attacks, financial fraud using stolen credit card information, and e-skimming where malware is injected in checkout pages to steal personal and payment information of clients (Seals, 2016). The U.S. Federal Bureau of Investigation noted that large online retailers that process orders online are at higher risk of e-skimming attacks (Schlesinger & Solomon, 2020).

Online customers, on the other hand, are vulnerable to phishing, spoofing, and online scams. For online scams alone, the DTI reported a fivefold increase from 2019 based on reports received by the agency from January to October 2020 (Porcalla, 2020). Similarly, the security firm Kaspersky reported a 158% increase in phishing attacks in the first quarter of 2020, targeting small Filipino businesses and exploiting the remote work setup (Esmael, 2020).

Email and email attachments remain the top vehicles for phishing and malware attacks (Gatefy, 2021). Many phishing attacks have exploited the COVID-19 pandemic, pretending to be government health ministries or health organizations. Also, with what seems to be endless sale events and holiday shopping, consumers always looking for the best deals could become victims of spoofed domains. Web email services like Google and Yahoo! are common targets as most user transactions are linked to their web email accounts.

Phishing sites are also continuously evolving. More phishing sites are using SSL certificates, creating a false sense of security.[29] Mobile phishing increased by 37% worldwide in 2020 (*Security Magazine*, 2020a) and increasingly targeted employees of pharmaceutical companies (*Security Magazine*, 2020b).

Cybersecurity as a Collective Responsibility

When it comes to cybersecurity, a strong defense is the best offense. As e-commerce operators that engage with Philippine customers necessarily process personal data, they are covered by the data protection and data security obligations imposed by the Data Privacy Act of 2012. This includes the implementation of reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against unlawful destruction, alteration, and disclosure.

As a best practice, e-commerce websites should have SSL certificates, and sites handling payment card information should be Payment Card Industry Data Security Standard (PCI-DSS) compliant. A website with an SSL certificate identified by a padlock logo gives an additional layer of security and creates a level of trust among shoppers. Information theft usually happens on unsecured vendor websites. In a 2020 report, Verizon noted that PCI-DSS compliance continues to decline, with only 27.9% of organizations worldwide being fully compliant, putting cardholders' data at risk (Verizon, 2020b).

Security experts generally advise implementing firewalls, utilizing strong passwords, and using multifactor authentication as security best practices. Employees of retail establishments must also be keenly aware of cybersecurity practices, especially as they use email and social media. Human error is often the cause of security breaches. Online retailers are advised to be especially vigilant during holiday shopping or sale events as cybercriminals usually use the high volume of traffic to mask malicious network activity (FireEye Inc., 2014). Companies implementing new payment systems are also common victims of threat actors seeking out security issues and vulnerabilities in the new system.

Customers should also adopt best practices and habits for themselves, such as shopping only on trusted sites, using only recognized and trusted payment services that offer fraud protection, avoiding virtual wallet transfers or direct money remittance payments that may not follow Know Your Customer rules, and never conducting online transactions using public Wi-Fi networks that are easy to intercept. Customers should be doubtful of offers that are too good to be true before clicking. The use of strong personal passwords is especially recommended. To increase protection from e-skimming, there are also banks that offer virtual credit cards and disposable credit card numbers designed for one-time payments.

Government-administered cybersecurity policies will also be critical to ensuring a safe e-commerce environment in the Philippines. Even without adopting or imposing technological solutions, government-run consumer awareness campaigns may already prove vital, especially if there are first-time users only starting to transition to digital transactions. Small businesses would especially benefit from government-provided cybersecurity guides that are easy to comprehend and implement.[30] The government, through agencies such as the DICT and the NPC, is likewise well positioned to provide periodic public information sharing on cyber threats and communicate the urgency of developing a clear crisis management plan in the event of a cybersecurity breach.

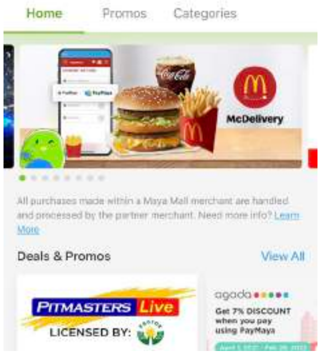
Electronic Banking and Financial Services

The Philippines is in the midst of fundamental changes ushered by the Internet on how commerce and business are conducted. By the end of 2020, the number of digital consumers in Southeast Asia will reach 310 million, or around 70% of the region's population (Facebook & Bain & Company, 2020). The COVID-19 lockdown has proven to be the ultimate stress test on a global scale in terms of business continuity and contingency planning. Going forward, businesses and governments will have to be able to offer their products and services with minimal to no physical and personal interaction.

This transition may widen the digital divide and exacerbate existing economic exclusion. In 2019, only 34.6% of adult Filipinos had formal bank accounts and less than 5% of the total population used digital payments regularly.[31] Despite this limitation, citizens were increasingly engaged in online transactions. A year before COVID-19 happened, a survey already showed increased online activity between January 2019 and January 2020, with 6% more adult Filipino respondents purchasing a product or service online and 9% more individuals purchasing online through a mobile device a year after (Kemp, 2021). From mid-March to August 2020, the DTI recorded an over 4,000% increase in business-name registrations for retail sale via the Internet, totaling 75,029 businesses registered as of September that year (Ramos, 2020c).

The country has seen the emergence of do-it-yourself e-commerce using simple tools like Google Forms and call backs, with payments facilitated by electronic money. It also helped that many banks and financial technology (fintech) companies waived their transaction fees during the pandemic. In contrast, brick-and-mortar banking was difficult, if not completely forbidden, during the lockdowns. To cope with a pandemic and other kinds of emergencies in the future, Internet banking will have to transition from being an alternative to becoming the primary banking channel.

These strides became evident during the first 45 days of the enhanced community quarantine, when BSP reported a 25% increase in online bank transactions, equivalent to 2.13 million more digital bank transfers, cumulatively worth PHP 64.62 billion (Lopez, 2020). The BSP and the banking associations have been working to enhance "frictionless" payments and settlements, which use digital platforms. InstaPay and PESONet, which are part of the National Retail Payment System, have been demonstrated as the first steps in this journey.[32] The BSP is also pushing for the use of a standardized quick response (QR) code format to help simplify the confusion brought about by multiple codes that need to be managed by retailers (Manuel, 2021).



All purchases made within a Maya Mall merchant are handled and processed by the partner merchant. Need more info? Learn More

Screenshot of PayMaya app

However, enhanced electronic banking offers limited solutions when many Filipinos are still unbanked. The growing use of electronic money may be what will drive financial inclusion in the country. In May 2020, for example, the number of GCash transactions was eight times higher than during the same period a year ago, according to a report by *Nikkei Asia* (Endo, 2020). Meanwhile, PayMaya offered fast-food chains end-to-end digital payments solutions for enterprise.[33] The government is also leading digital adoption efforts with both national and local governments tapping into mobile wallets to distribute cash aid to beneficiaries.

Without digital payments and settlements, e-commerce and e-government would be ad hoc and incoherent. The need for and urgency to establish a seamless payments and settlements regime must be viewed through the lens of public interest. And in an increasingly digital world, customer protection must now include digital rights, information security, and data privacy.

Creating a Secure and Seamless Digital Payments Ecosystem

What should a seamless settlements and payments environment look like? The following key features are essential:

- **Pervasive.** Business and government occur throughout the Philippine archipelago, not just in urbanized areas. Unless digital payments are made easy to use and widely available and accepted, cash will remain the preferred form of payment.
- **Inclusive and nondiscriminatory.** The survival of micro, small, and medium-sized enterprises (MSMEs) will be determined by their ability to send or receive digital payments. This also means that it should be affordable enough for small businesses to adopt. Clearinghouses and payment networks must make the services equally available to all parties under fair, reasonable, and nondiscriminatory (FRAND) terms to avoid creating protectionist bubbles.

- **Interoperable.** Users should not have to maintain multiple digital accounts or wallets nor deal with multiple protocols, codes, and formats. Interoperability allows merchants to subscribe to one payment network that can be linked to others.
- **Reliable.** The platforms must be available, consistent, and secure. Users quickly stop using a new technology offering if they are unsuccessful in executing their transactions after a few tries.
- **Safe and secure.** As an equally important feature of any digital payments solutions, the platforms used by customers, financial institutions, MSMEs, and the government in making contactless transactions must be equipped with a system capacity that is free from any digital threats that may compromise the transactions or put the user accounts at risk for fraudulent and hacking activities (Better than Cash Alliance, n.d.; Goosen, 2017).

These features may not be achieved immediately, but it is crucial that policy and regulations allow innovation to take its course. The BSP has cited the use of a regulatory sandbox approach to digital financial services to support growth of digital players and address potential risks. The BSP "openly engages with fintech players and innovators through a flexible 'test and learn' environment, or the 'regulatory sandbox' that enables [the BSP] to fully understand emerging business models while assessing attendant risks.[34]"

Such a seamless digital environment instantly becomes a more tempting target for fraudsters due to the multiple end nodes and data bridges that a payment or settlement authorization has to traverse. This interconnected web creates a larger attack surface.

Unfortunately, any decision to relax interoperability and seamless processing of settlement will result in a fragmented and inefficient environment, which requires the billers and payers to transact using the same exact payment service provider (BSP, 2020a). This means more layers of processes, more cost, and less access to digital payments for some segments of society who will be using manual payments.

Fragmentation will also mean a multitrack economy where entities that can be accommodated by the fragmented settlements environment will be more efficient and experience less business disruption, which will introduce a competition bias. This may also reduce the attractiveness of e-money if the average citizen is forced to divide their limited, hard-earned cash into multiple wallets.

A digital business-to-business transaction is a process consisting of at least two digital steps: (1) creation of an enforceable digital contract that accommodates digital payments; and (2) recognition by the bank of the digital transaction. For the time being, the only seamless transaction done by banks is the payment of monthly utility bills, which is merely a citizen-to-business transaction.

To address this, the BSP is pushing for the establishment of an integrated bills payment facility (Agcaoili, 2020). There are very few instances that can compare with this pivotal shift in approaching settlements and payments in terms of its potential to reset the entire economic and business landscape.

Security Threats and Challenges

Common security threats to e-commerce and online banking include information leakage and identify theft, transaction fraud (such as the Nigerian prince email scams, outright theft of funds and investments, and fake transactions), malware attacks, and various phishing schemes.

Banks are clearly not immune to attacks. One recent case in the Philippines is the PHP 167-million United Coconut Planters Bank (UCPB) cyber heist. Cybercriminals managed to steal huge sums of money through a malware that was inserted into the system when UCPB was implementing a security upgrade to its 2-decade-old IT system (Lucas, 2020).

Phishing and spoofing have also risen during the pandemic, as fraudsters take advantage of government aid programs and other forms of assistance (O'Flaherty, 2020). Email spoofing is when a fraudster forges the sender address and mimics a legitimate website. Unsuspecting account holders' sensitive information is stolen once they log in to the mimicked sites.

In 2020, BSP issued Memorandum No. 2020-066 advising banks of growing SMS-based phishing or smishing attacks and to ramp up their security protocols (BSP, 2020d). With smishing, fake text messages are sent as advisories from banks or digital payment services, asking clients for their login details through text message or by clicking a malicious link.

Securing Online Transactions

Financial institutions have heavily invested in keeping their security systems tight and up to date. Technologies like machine learning and artificial intelligence are used to improve detection of fraudulent activities. Banks use area denial campaigns that limit the risk of fraud, such as by disabling certain features on an Internet banking website but still allowing it on the application version of the service. While this effectively reduces the fraud space to the custom application, approaches like this are temporary and may sacrifice user experience for security. It also goes against the objective of making fintech services available in all devices and modalities at all times.

Banks and e-commerce sites also use security features such as multifactor authentications and two-step verification, which require customers to use at least one more method to verify their identity.

On the consumer end, awareness and education are essential. Banks and digital payment providers will never ask for login details through calls, text message, or email. Consumers should be suspicious of messages requiring urgent action. They should also investigate e-commerce sites, check the reviews, understand the product description, and always remember to log out. Anyone working online should practice good cyber hygiene habits, like ensuring that laptop and mobile phone operating systems and applications are updated regularly and avoiding the use of shared networks and devices when doing online transactions.

Several laws have been passed by Congress to protect peoples' digital lives as they access electronic financial services, including the Data Privacy Act, Cybercrime Prevention Act, and Access Devices Regulation Act. Under the e-Commerce Act, existing laws such as the Consumer Act also apply to e-commerce transactions.

For its part, the BSP employs a flexible "test-and-learn approach" to the banking industry's digital transformation. This approach is seen to encourage innovation, mitigate risks, and ensure risk-based regulation.

The BSP's policies are critical to the success of e-commerce in the Philippines. The BSP has declared financial inclusion as part of its policy (Tetangco, 2015). Under the shadow of the pandemic, it is critical that all sectors of society have access to digital payments. The BSP also has authority over the telcos who applied for licenses as electronic money issuers. It should follow that BSP enforce its policy and require the likes of GCash and PayMaya to be seamlessly interoperable.

In this case, there is an overlap of authority between the NTC, which regulates the telcos, and the BSP, which regulates financial services, including digital wallets. The NTC and the BSP should agree in equating interoperability of digital wallets to serving the public interest.

It is expected that online transactions will continue to be the norm even after the pandemic. Therefore, aside from an enabling legal environment, reliable Internet infrastructure must be in place.[35] Despite the promise offered by enhanced electronic payments and digital trade portals, the very lack of reliable Internet connectivity and access by many Filipinos may be a bottleneck to the development of e-commerce and Internet banking in the country.

Healthcare Management

Digital technology has allowed for enhanced provision of health services. It has enabled innovations such as teletriage and telemedicine,[36] allowed for more effective monitoring of cases in rural and remote areas, and facilitated greater coordination and access to information by healthcare professionals. This dependence on digital technology, however, has exposed several issues—from data privacy concerns over telemedicine and contact-tracing apps, to cyberattacks on critical institutions (e.g., hospitals and government agencies), to phishing or impersonation of trusted organizations.

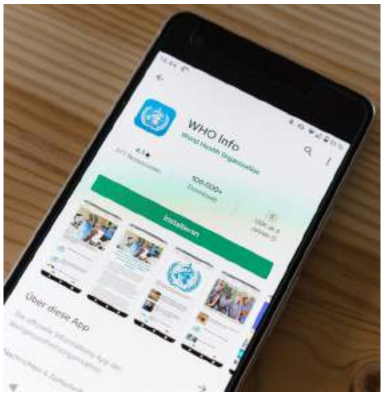
Cybersecurity risks pose multiple threats to the healthcare infrastructure of the Philippines.

Cyberattacks directed at healthcare providers, or public–private medical insurance providers, could impair the direct and timely delivery of healthcare to patients. Highly sensitive medical information of individuals could likewise be compromised on account of cyberattacks. The degree of damage that cyberattacks could have on the Philippine healthcare system and its providers heightens the need for consciousness and action to mitigate these risks through effective cybersecurity.

Cyberattacks on Health Institutions

With the uncertainty brought about by the coronavirus pandemic, people are constantly looking for reliable sources of information about COVID-19. This has made critical institutions prone to cyberattacks. Trusted organizations, such as the World Health Organization (WHO) or the United Kingdom's National Health Service, have become targets of phishing and other cybercrimes. Even crimes such as industrial espionage are increasingly becoming digital in nature (Corera, 2020).

At the start of the pandemic in April 2020, 450 active WHO email addresses and passwords were leaked online. According to the WHO (2020), the leaked credentials belonged to individuals working on COVID-19 response. In May that same year, over 100 users of the National Health Service's email system received phishing emails, which turned to be part of a global phishing campaign targeting many organizations (Scroxton, 2020). Health institutions have been used by scammers for fake donation schemes. Online scammers have also impersonated the WHO in emails soliciting donations to fake COVID-19 response funds (Stupp, 2020).



In April 2020, the International Criminal Police Organization (Interpol, 2020a) issued a warning to critical healthcare institutions as it detected a rise in ransomware attacks. It also alerted police from all its member countries to provide information on the modes of operation and hiding places of cybercriminals amid increasing cyber threats.

The usual scheme of cybercriminals is to steal confidential information from companies and organizations and threaten to publish them, unless the organizations pay ransom fees (Stupp, 2020). In the United Kingdom and the United States, reports of foreign government-backed hackers targeting pharmaceutical companies and research institutions have proliferated. According to the U.K. National Cybersecurity Center and the U.S. Cybersecurity and Infrastructure Security Agency, hackers have attempted to obtain intelligence on national and international healthcare policy and data on COVID research (Stubbs & Bing, 2020).

Two conditions have made it easier for cybercriminals to operate: First, hospitals and healthcare institutions are now more exposed online, thus making them easier to attack. Second, institutions that are in critical condition (i.e., hospitals with a high number of patients with COVID) have minimal time to negotiate with hackers.

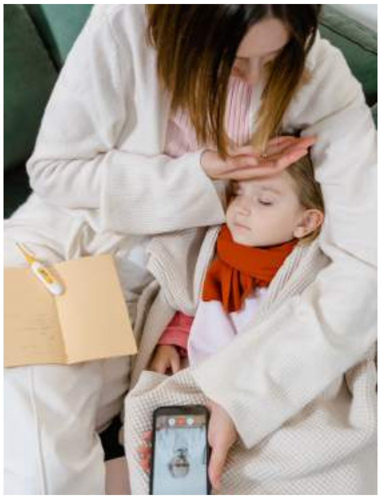
From these attacks, it can be inferred that hackers and scammers exploit these health institutions because of their credibility to the public. It is easier to trick people into donating or providing personal information to institutions that they trust. Apart from healthcare institutions being victims themselves, bad actors have used the credibility of these organizations as a front for phishing attacks with the aim to steal information, inject malware as a vector for further attacks, or just execute plain vandalism. During the pandemic, people are likely to click on a link from an email from credible sources, like healthcare institutions. There are even cases where the information is actually accurate and replayed from credible sources to bait unwitting victims.

Defense Against Cyberattacks on Health Institutions

Cybersecurity experts advise that hospitals and healthcare systems put a premium on protecting patient data. Organizations need to implement regulations and standards, such as putting up firewalls and boundary security, securing configurations, installing malware protection, and ensuring authentication mechanisms when patients provide information (Ghebreyesus, 2020). Hospital staff should also avoid posting too much information about their professional roles on social media to avoid being targets of cybercriminals (Jercich, 2020).

In Europe, the European Union Agency for Cybersecurity (ENISA) issued procurement guidelines for cybersecurity in hospitals, including good practices for the procurement of healthcare assets, products, service, industry standards, and cybersecurity challenges. ENISA identified the vulnerable nature of medical devices such as CT scanners or MRI machines designed to support remote patching and firmware updating, which could create security loopholes (ENISA, 2020).

Privacy Concerns and Telemedicine



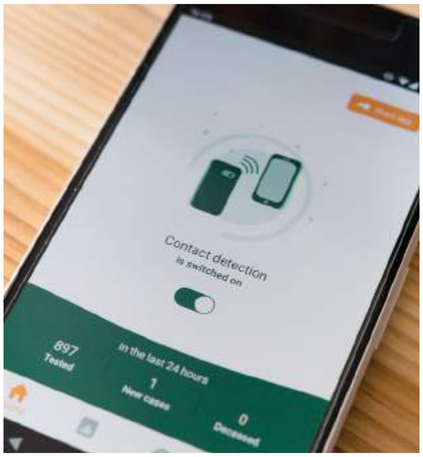
The need to observe physical distancing has limited access even to medical services. Due to the highly contagious nature of COVID, it has become difficult, and even discouraged, to go to hospitals for consultations and other non-COVID health concerns. Telemedicine plays a crucial role in delivering remote diagnostic and medical care as an alternative to traditional in-person consultations, thus helping reduce the spread of the virus. It allows patients who cannot immediately go to hospitals or those who live in far-flung areas to still get some form of medical care. Telemedicine also helps prevent overcrowding and depletion of resources, especially in hospitals with critical capacity.

Patients can teleconsult with healthcare professionals through phone calls or by using online platforms like Viber, Facebook, Messenger, and FaceTime (ABS-CBN News, 2020a). This is where the handling of patients' data by teleconsulting facilities becomes a key issue. By agreeing to undergo a teleconsultation session, patients are often asked to provide personally identifiable information, such as their name, birthday, email address, and medical history. Whenever necessary and possible, patients are also asked to send photos of the medical condition being reported.

In the Philippines, the Data Privacy Act requires the data controllers to put in place security measures for the protection of processed personal data (i.e., preventing unauthorized access to data, using privacy-enhancing software, and using effective authentication processes like passwords and automatic logout), which would apply to telemedicine.

The University of the Philippines National Telehealth Service Program advocates for medical privacy and patient information confidentiality, and for telemedicine services to abide by the DPA. This involves getting the consent of the patient prior to the consultation and recording of the session (Patdu & Tenorio, 2016; National Institutes of Health, n.d.). Private teleconsulting services in the country have established policies that explain the collection, usage, storage, sharing, and protection of personal information (Medgate Philippines, 2018).

Privacy Concerns over Contact-Tracing Apps



Aside from phishing attacks, data privacy issues over contact-tracing apps employed during the COVID-19 pandemic have also emerged. Several countries have started to test and launch contact-tracing apps to identify users who have tested positive for COVID-19 and to trace those with whom they have been in close physical contact. Singapore rolled out its contact-tracing app called TraceTogether, Australia launched COVIDSafe, and Germany launched Corona Warn as the European Union began to relax travel restrictions (Lyons, 2020a).

Contact-tracing apps use telecommunications data, GPS, and/or Bluetooth technology to gather data when users are in close proximity with each other. Once a user reports COVID-like symptoms to the app, it will trace the people that the user came in contact with and provide the proper notifications to both the concerned parties and the authorities. Although these apps make it faster and more efficient for governments to detect potential cases and to notify citizens if they need to self-isolate, there have been growing concerns about data privacy.

Government Frameworks for Addressing Privacy Issues

A framework for the use of contact-tracing apps has been established by the EU, which developed a “common toolbox” for its member states (European Commission, 2020). The main principles in this framework include (1) accountability of public health authorities for the approved apps, including their data; (2) guaranteed interoperability of apps across member states;[37] (3) transparency of app developers with how they will use the data shared on contact tracing apps; and (4) retention of data only during the course of the pandemic.

The United Kingdom has also developed a set of guidelines on data protection specific to contact-tracing apps (Information Commissioner's Office, 2020). The key principles are transparency about the purpose, design choices, and benefits of the app; collection of the minimum amount of personal data; and user protection.

The U.S. National Institute of Standards and Technology (NIST) works with a cross-laboratory group to use their expertise in privacy, cybersecurity, and measurement-science fields to develop and meet the challenges of using contact-tracing apps (NIST, 2020).

In the Philippines, the DPA would require from contact-tracing app developers clarity on the purpose of data collection. The DPA provides that data collection must be based on proportionality, which means that the "processing of personal information must be relevant to, and must not exceed, the declared purpose."

The government's Inter-Agency Task Force on Emerging Infectious Diseases (IATF-EID) adopted StaySafe as the country's "official social-distancing, health-condition-reporting, and contact-tracing system that will assist in the government's response to COVID-19" (IATF, 2020). However, questions have been raised about data privacy, data ownership, and the effectiveness of the app. The app has been characterized as "a health monitoring app with a location tracker," but with "no contact tracing capability" (*Inquirer*, 2021). Notably, the StaySafe app may access geolocation (if enabled), device information, and browser activity (StaySafe, 2020).

In response to these issues, the IATF issued Resolution No. 45 in June 2020 directing Multisys Technology Corporation, StaySafe.PH's developer, to enter into an agreement with and donate the app to the Department of Health (DOH). The donation should include the app's source code, all data, data ownership, and intellectual property, with the requirement that all data collected would be migrated to DOH's COVID-Kaya system. Multisys was given 30 days to comply with the directive.

To help governments navigate through the challenges of using contact-tracing apps, Apple and Google have set up privacy-preserving contact tracing with data security at the center of its design (Apple Newsroom, 2020). This service will only be made available to one nominated app per country, which, in the Philippines' case, is the StaySafe app. This may help assuage some of the concerns about the large amount of sensitive information being collected and shared during contact tracing. With this approach, application developers outside of Apple and Google will not get information unnecessarily.

Toward a More Cybersecure Health Sector

Regardless of the technology or platform used, there is a globally accepted set of principles on how app developers should responsibly use patients' data (Patdu, 2020). Apps must inform users of the privacy risks, keep personal information confidential, use the data for medical purposes only, and ensure that the information is secure, especially when saving it in electronic devices. Data ownership is of utmost importance and must be clarified to ensure the app users' right to privacy. After data is collected by the app, to whom does it belong? Will the app developers be allowed to use the data for commercial purposes?

> **With the expected increase in the use of digital technology going forward, institutions need to invest now in improving cybersecurity measures to protect their systems and networks.**

This public health emergency has forced everyone to weigh privacy against public interest. This is true for initiatives such as contact tracing and mandatory information disclosures for visiting establishments such as restaurants, stores, and other venues.[38] Not all establishments and organizations are used or even equipped to collect, handle, and protect personal information. Hence, it is critical that a balance be found. Educating both users and organizations is necessary to ensure that people's privacy rights are protected during and beyond the pandemic.

With the expected increase in the use of digital technology going forward, institutions need to invest now in improving cybersecurity measures to protect their systems and networks. COVID-19 has exposed the vulnerabilities of healthcare and government systems. If anything, this pandemic should serve as a cautionary tale. It is important for nations to establish and strengthen the frameworks for data protection, ownership, and management in preparation for another crisis in the future.

Energy Resources Management

Over the past decade, digital technologies have greatly contributed to the development of more efficient, reliable, and sustainable energy systems around the world. Intelligent systems have been used to improve accessibility, safety, connectivity, and productivity in the energy sector. These trends operate within the purview of the energy Internet of Things (IoT), which can be described as a result of the convergence and digitalization of operational technology and information technology (Mylrea, 2017).

The energy sector is also one of the earliest users of machine-to-machine technology that underpins the energy IoT in the form of supervisory control and data acquisition (SCADA) systems. These technological advancements, however, have also made the critical energy infrastructures vulnerable to cyber threats. Given that many other industries rely on the energy sector for the delivery of critical services, there is a need to understand the ways in which the acceleration and transition of technologies in energy infrastructures have brought about not only opportunities but also challenges in terms of vulnerabilities to cyberattacks.

In terms of opportunities, the increased digitalization of the energy systems and infrastructures have opened new services and markets, including growth in the use of renewable energy resources, two-way grid communications, and machine-based learning. These "smart" energy technologies have also produced new features, such as smart meters, grids, and appliances. The use of smart meters has allowed the introduction of net metering, which is fueling deployments of solar, biomass, and alternative power systems. Many countries have also shifted from traditional meters to smart meters as they provide utility companies and consumers with a detailed look at their energy usage. Real-time energy marketplaces have allowed consumers to diversify their power sources and give them an option to procure more green power.

In addition, the increased digitalization of power systems has optimized energy value chains (i.e., generation, transmission, distribution, and consumption), which have made buildings, cities, communication lines, and critical infrastructures more connected, effective, and sustainable. These innovations have not only dramatically reduced the amount of labor needed but also allowed direct savings and investments toward environmentally friendly technologies.

Notwithstanding the gains from these technological developments, the convergence of energy systems and cyberspaces has also created multiple layers of threats and risks that need to be mitigated. Cybersecurity issues related to energy can be applied to subsectors such as oil and gas, electricity, and nuclear power. Renewable energy resources like solar and wind power also require two-way digital controls, which heighten cyber vulnerability and require protection.

In light of these contexts, what are the threats and challenges accompanying the energy sector's reliance on digital technologies, especially in the Philippines? Who are the stakeholders involved in the interplay between energy and cybersecurity? What can be done to mitigate the threats facing energy systems?

Threats, Vulnerabilities, and Actors

An early sign of the possible risks that the Philippines may see more of in the future was a complaint filed in the 2000s by Meralco with the NTC, alleging that newly deployed Wi-Fi and near-Wi-Fi systems were interfering with their wireless SCADA platforms. The complaint clearly mentioned that the use of these wireless technologies could compromise wireless systems and possibly cause system failures and blackouts. This demonstrates a means by which power distribution systems can be intentionally disrupted, leading to a denial of service.

In December 2015, in the Ivano-Frankivsk region of Ukraine, hackers reportedly sabotaged the equipment of power distribution firms Prykarpattya Oblenergo and Kyiv Oblenergo by using a novel malware, which affected 225,000 consumers (Reuters, 2016). This incident demonstrated that cybersecurity is critical in preserving the integrity and correct operation of power systems and in protecting the safety and welfare of citizens.

Compared to conventional threats to electrical grids, such as severe weather conditions, cyber threats are proving much harder to anticipate and address. Security experts have identified electric power and gas companies as the most vulnerable to cyber-related risks (Bronk, 2014). Proper management of energy distribution systems requires a perfect balance between supply and demand. If too much supply is taken off the grid or too much demand comes up all at once, grids may fail and cause massive outages. In this regard, the SCADA systems play an important role in ensuring that the grid frequencies are properly maintained. Much like in electricity, critical information infrastructure is also necessary for the production, transportation, refinement, and distribution of oil and gas.

In 2013, a report from the Council on Foreign Relations (Clayton & Segal, 2013, p. 2) explained:

> [A] major risk facing the oil and gas industry is the disruption of critical business or physical operations by attacks on networks. As information technology's role in all phases of oil and gas production—from exploration and production to processing and delivery—expands, the vulnerability of industry operations to cyberattacks increases. A hacker with the right tools, access, and knowledge could, for instance, identify the Supervisory Control and Data Acquisition systems (SCADA) and industrial control systems (ICS) used to operate critical infrastructure and facilities in the oil and gas industry and that are connected to the Internet.

The dynamic and fluid changes in the virtual environment make the threats and risks confronting the energy sector more complex. Cyber incidents can lead to loss of grid control, personal data theft, firmware, and data exfiltration, among others. In the power industry, several threats can be found in the generation, transmission, distribution, and network.

Some potential examples of system compromise may include (1) grid failure or denial of service; (2) catastrophic failure such as meltdowns or plant destruction; (3) energy system trading arbitrage (i.e., bankrupting a plant by making it appear unable to produce more than it should, valuating a plant higher than it really is, or manipulating the market); and (4) data theft. The possible impacts can include ransomware attacks against power plants and clean energy generators, widespread power disruption by remotely disconnecting services, disruption of local and regional stations, and information theft (Bailey et al., 2020). Cyberattacks, therefore, affect utilities across the entire value chain.

The source of threats can involve a wide range of state and nonstate actors, including cybercriminals, hacktivists, cyber syndicates, ecoterrorists, common thieves, script kiddies, and terrorists. In most cases, the use of computers and other ICT devices can exacerbate the impact of traditional crimes. In some cases, hacktivist groups also use web defacement tactics or malware attacks. They can also target utilities using publicly available attacks, such as a DDoS. In December 2020, a massive data breach, for instance, was discovered against the U.S. Department of Energy and National Nuclear Security Administration as part of the suspected activities of Russian intelligence operatives (Bertrand & Wolff, 2020). There also have been concerns about the possibility of cyber-related attacks on critical infrastructure, such as nuclear, dams, and gas (Counter-Terrorism Committee Executive Directorate, 2017).

The U.S. government has warned that countries that are "capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure" can use the cyberspace as a tool to deter attacks or retaliate against their adversaries due to geopolitical and terrorism threats (U.S. Department of Homeland Security, 2020). In the United Kingdom, the threat of cyberattacks has also generated considerable concern. Lord Arbuthnot of Edrom, former chair of the House of Commons Defense Committee, expressed that securing the power grids is essential: "If you take down the electricity network, you very quickly take down everything else as well. The vulnerability is real" (Pfeifer et al., 2018). The Swiss Cyber Forum (2020), meanwhile, cites three reasons for the vulnerability of the energy sector to cyberattacks: (1) the rapid pace of technological innovation; (2) the increasing sophistication of cyberattacks; and (3) the sector's attractiveness as a cyber target.

While it seems that developed countries are more prone to cyberattacks, developing countries such as the Philippines may also be dragged into the cyber warfare between great powers or into geopolitical disputes against neighboring countries. The latter was raised at a Senate hearing in 2020 about the State Grid Corporation of China's 40% ownership of the National Grid Corporation of the Philippines, which alarmed security experts given the country's dispute with China over the West Philippine Sea (South China Sea) (Ramos, 2020a). The growing anxiety among Filipino policymakers about potential cyberattacks on the nation's energy infrastructure was encapsulated in a statement by Senator Sherwin Gatchalian (Griffiths, 2019):

> I was advised by the president of TransCo [National Transmission Corporation] that they have studied this type of possibility. I was advised that manual operation of transmission lines is possible. A takeover can happen, but TransCo, with their technical capability, can then manually take over.... With a single switch, no electricity would be transmitted to any of our homes, our businesses, (or) any of our military facilities.

Senator Risa Hontiveros also warned that "as long as the system operations are controlled and managed by Chinese engineers [they have] an enormous power" over the Philippine energy supply (Everington, 2019). Given the interconnected nature of energy systems, critical infrastructure represents a national security vulnerability that is not directly within the purview of the government. The Philippines needs to prepare to respond to, and recover from, cyberattacks on power infrastructure, which have cascading consequences on various other sectors.

Challenges in Building Capacities for Cyber Preparedness

Major cybersecurity initiatives and forums around the world have underscored the need to strengthen capacities to digitally secure energy systems, especially as cyber threats become more sophisticated and frequent. There is also a growing deployment of new digital devices that can introduce greater forms of cyberattacks.

Securing energy systems entails securing the whole ecosystem—producers, distributors, and major consumers across the grid. Any of these players can be used to compromise the whole grid due to the interconnected nature of power systems, which is necessary for balancing electricity supply and demand in real time.

In light of the networked nature of the digital environment, the Energy Expert Cyber Security Platform (EECSP) has identified the main challenges of building cybersecurity preparedness in the energy sector, which include grid stability in a cross-border interconnected energy network; the handling of cyberattacks within regional bodies like the EU and the ASEAN; the introduction of new, highly interconnected technologies and services; and the availability of human resources and their competencies, among others (EECSP Expert Group, 2017).

Another problem is potentially exposing extensive usage data to utilities and third-party firms, not only for billing time-of-use but also for guidance on profiling, settlement, forecasting, tariff, and energy efficiency (Mylrea, 2017, p. 149). This becomes more problematic due to the different stakeholders that need to be considered such as Internet service providers (ISPs), third-party energy generators, and sellers of smart energy technology. Deployment of technological solutions in energy needs to be done with the data privacy of consumers in mind.

Fostering Cyber Resilience in the Philippine Energy Sector

The different threats and challenges confronting the energy sector will most likely persist for many decades. For the Philippines, it is also imperative to consider the ways in which energy stakeholders can produce resilient systems and minimize the consequences of cyber incidents. These threats are real, with multiple actors seeking to enter some of the most secure energy structures. While energy sector stakeholders generally recognize the vulnerability caused by increasing dependence on digital technologies and networks, fostering cyber resilience in the energy sector demands changes in the priorities of governments and businesses. While interoperable solutions require common standards, cybersecurity can be viewed from alternative standpoints, which require the development of holistic models to address the cyber-related issues facing the energy sector. Cyber resilience of critical infrastructure should be elevated as an important action point within the national security agenda of the country.

The Philippine Department of Energy (DOE) recognizes that the vulnerability of the transmission grid system from cyberattacks is a growing national security concern (DOE, 2021, p. 226). Thus, Department Circular No. 2020-02-0003 requires that generation companies, distribution utilities, and transmission network providers develop a cybersecurity infrastructure that is compliant with all relevant laws and regulations as well as internationally accepted standards at the appropriate level of adoption and application (Sec. 5.7). Philippine industry players should foster and share their best practices in securing their systems from cyber threats. Although larger industry players have more resources to protect themselves than smaller players, the former are still made vulnerable if the latter are not able to secure their systems. As such, it is imperative for the entire ecosystem to share their practices for the benefit of the entire sector. This is particularly true for energy distributors and utility services. There should be multisectoral initiatives aimed at improving the visibility of cyber threats, such as the establishment and utilization of sector-based CERTs, which have been promoted by the DICT in its policy issuances.[39] These sectoral CERTs can also create linkages with other international partners, creating better shared visibility of potential issues. In addition, there is also a need to ensure the country's critical infrastructure is not vulnerable to foreign interference. Proper control management and isolation must be put in place to ensure that the Philippine government is able to maintain sovereign control of critical information infrastructure (CII) systems at all times.

Cyber-related incidents should be treated not only from the perspective of organizations but also from the viewpoint of cross-cutting issues and sectors that impinge on the interconnected energy supply chain. Given the goal of many countries like the Philippines to transition from nonrenewable to renewable energy, utilities and nonutilities should have contingency planning to contain and minimize the impacts of cyber and physical incidents. The government and industry stakeholders must recognize the vulnerabilities posed by the interdependence of virtual and physical infrastructures. This can be done through cyber risk intelligence and the monitoring and analysis of the potential compromises in the energy systems.

Water Resource Management

The Philippines, with 421 water basins, is rich with naturally occurring fresh water. But access to water supply could be variable, with factors such as deforestation, uneven rainfall, changing climate, and natural catchment areas that determine water availability in different areas.

Water resources management and governance is thus very critical. The water sector includes potable water, water for agriculture, water for energy (dams), and wastewater management systems. It is considered critical infrastructure as it directly affects public health, food security, and national security. Water systems are vulnerable to a variety of threats, such as natural disasters, physical attacks, and cyberattacks. Disruption of water service, accidental spillage, contamination of water systems, or manipulation of control systems could widely impact economic, environmental, and public health spheres. The water sector is also dependent and interdependent on other critical infrastructures, such as energy, transportation, food, and emergency services (e.g., hospitals, firefighting).

The water sector also faces numerous complex challenges, such as water shortages, weather and climate change, natural disasters, and infrastructure obsolescence. The use of technology brings to the table a number of solutions that can improve water use efficiency and management. However, with new technology, new vulnerabilities are exposed.

Here are some of the key areas for consideration for the protection of critical water infrastructure in the Philippines.

Control Systems

Water supply and distribution use ICS that monitor and control industrial processes. These are typically called SCADA systems. An ICS is composed of various programmable logic controllers or discrete process control systems that control various aspects of the system from measuring key indicators like pressure in a distribution system or salinity in a saltwater conversion facility. These systems also provide automatic control for certain tasks like ensuring proper acidity levels by adjusting mixtures of chemical additives. These SCADA systems provide numerous facilities to monitor and control utilities. They are used to gather real-time information, such as pH level, chlorine content, water intake, turbidity, and water pressure from various equipment in the utility, and to transmit these to a central site or to a control room. The information allows water managers to make critical decisions with respect to the state of the network, such as maintaining smooth operations and detecting inefficiencies and possible leaks, among others.

The consequences of compromised control systems can range from trivial to fatal. One of the biggest incidents involving a SCADA happened a decade ago. The so-called Stuxnet attack compromised Iran’s Nantanz nuclear power facility’s centrifuges (Bosse, 2020). As an unintended consequence, the Stuxnet malware did not just stay in Iran but spread throughout the world, causing substantial damage to many other systems in many other countries.

For water networks, a compromised SCADA could potentially harm a whole population. In 2020, Israel confirmed at least three cyberattacks in their water management facilities linked to Iran. The first attack in April tried to control the chlorine levels in its water treatment systems, potentially poisoning crops, livestock, and people. The second one struck at agricultural water pumps, aiming to disrupt critical irrigation for crops. The third attack targeted water pumps, aiming to disrupt retail water supply. All were detected and addressed before causing any harm. If successful, these attacks would have led to significant economic and health repercussions.

In 2021, the water utility control systems in Oldsmar City in Florida, United States, were compromised when a hacker reportedly manipulated the level of sodium hydroxide in the water supply from 100 ppm to 11,100 ppm (Greenberg, 2021). Had it not been detected early, this “extremely dangerous” level of sodium hydroxide could have poisoned the water supply for the citizens of Oldsmar.

Connectivity and Networks

With the introduction of new technologies, industrial control systems and operations are migrating from old forms of communication methods to ethernet networks or 4G and 5G networks (Boubaker, 2020). This makes industrial systems interconnected and allows access anytime and anywhere, both for operators and potential hackers. As water and other industrial systems increasingly rely on ICSs and 5Gs, which have taken on more capabilities over the years, cybersecurity risks are increasingly possible.

Increasingly, network managers are dependent on real-time information from these distributed SCADA systems. If the communications networks of these distributed components are compromised, the resulting delay in the receipt of information could have severe consequences. It is also possible that bad actors or unscrupulous groups could execute a perfectly timed disruption on some of these communications links to manipulate the behavior of these water systems.

Data and Information

A cyberattack may have diverse motives—from a hacker infiltrating a system to steal data, to sophisticated attacks that can gain access to halt systems, to control flood gates, or to control industrial settings to cause water contamination. In an Iran-linked attack in 2013, bad actors hacked the command-and-control system of a small-scale dam in New York through a cellular modem (Thompson, 2016). This attack provided access to critical information about that dam that could be used for subsequent attacks. Fortunately, remote access to the sluice gate of the dam was disabled, preventing a more kinetic form of compromise. In 2018, Russian hackers reportedly targeted Ukraine’s water supply but was successfully thwarted by authorities (Martin, 2018).

Most critical infrastructure attacks are sophisticated by nature. Incident response may also take time. A study shows that, on average, it takes 80 days to detect a malicious cyber breach and another 123 days to resolve it (Clark et al., 2017). A system can then be compromised for 6 months on average.

Philippine Water Sector: Issues and Challenges

In the Philippines, the DICT has ongoing efforts to set up a sectoral CERT for critical infrastructure. Currently, there is no public data on attempts made in the water sector or measures in place to ensure that mechanisms are present to secure this critical infrastructure. The current legal and institutional framework may impose challenges for strengthening information security.

Complex Legal Framework. The Water Code of the Philippines (1976) is the main law that governs water access, allocation, and utilization. It stipulates that domestic water use should be prioritized over other uses, such as irrigation, agriculture, or industrial use. There are, however, at least eight laws that provide a framework for the water sector; this complicates how decisions are made.[40]

There are inconsistencies in the ownership and use of water resources stipulated in certain laws. For example, the Water Code states that "all water belongs to the state." However, the Indigenous People's Rights Act protects the rights of Indigenous people over their ancestral domain, including water resources. The absence of clearly defined legal ownership rights over particular water resources may hamper the institution of necessary cybersecurity measures.

Fragmented Water Institutions. The hydrological cycle and use of water is diverse, including water supply and sanitation, irrigation, industrial use, energy generation (dams), flood management, and watershed management. In the Philippines, more than 30 agencies[41] have overlapping mandates on water governance. Water planning and coordination, for instance, is shared by the NEDA, National Water Resources Board (NWRB), and LGUs. Water supply and distribution is under NWRB, Local Water Utilities Administration, the Department of Interior and Local Government (DILG) and LGU-led community water systems, or water districts. There is a multiplicity of institutions, organizations, and regulations governing water.

The existing setup has evolved because different water uses were fitted against existing agency mandates. Thus, the responsibility to oversee the security of this critical infrastructure is also divided among several agencies.

There are legislative efforts to address these issues. A bill is pending in Congress to create the Department of Water Resources, which shall be the primary agency responsible for the country's water resources. Considered a priority measure of President Duterte, this bill was approved by the House Committee on Appropriations last November 2020 (Cervantes, 2020a). In the meantime, water governance remains fragmented. This potential consolidation could help guide service providers with respect to handling new technologies and new vulnerabilities. The potential sharing of best practices and risks will benefit the entire industry.

Capacities of Water Utilities. In Metro Manila, there are only two water service providers (WSPs). For the rest of the country, there are at least a thousand WSPs providing piped or Level III water systems. Estimates range from 1,000 to 6,000 WSPs (Asia Development Bank, 2013, p. 3). These WSPs range from LGU-owned and operated water utilities, water districts, private sector operators, and small-scale community-based organizations. WSPs have different water control systems, varying levels of automation, and resources. Risk management plans and policies must be adopted to meet each WSP's security and organizational requirements. Each of these thousands of WSPs will have different levels of capability to handle emerging threats.

The importance of the sector was highlighted in March 2019 when water shortages and interruptions hit around 10,000 households in Metro Manila. The water level at La Mesa Dam was below the critical level due to El Niño. By April 2019, the Department of Agriculture estimated production losses to PHP 7.6 billion, affecting 247,610 farmers and fisherfolk due to the water shortage (Mogato, 2019).

The need for increased security in critical infrastructure is not theoretical. In 2015, Abu Sayyaf successfully bombed a pipeline in the southern province of Basilan, which caused a water outage for 5 days (Glang & Ramos, 2015). A second attempt to plant an explosive device was caught in time. These incidents show that water security and resilience need to be taken seriously. This is denial of service, albeit physical in nature.

Protecting the Water Infrastructure

As industrial control systems transition to new and increasingly connected technologies, the risk involved in the operation of things must expand from natural, climate, and disaster-related risks to include cyber risks as a permanent fixture in risk management. The design, operation and maintenance of control systems must ensure resilience against all attacks, including cyberattacks.

The bigger WSPs are likely to capitalize on new technology and address the ever-increasing and complex threat landscape. However, the many smaller thousands of WSPs will not have the same resources as the bigger ones. There is an opportunity to open up capabilities to these smaller WSPs that together cover a larger portion of our water assets. Strong leadership in this sector is needed.

Recognizing the vulnerabilities and the potential consequences in the country's water sector should be clearly communicated to the nation's leaders to establish a sense of urgency to secure our systems. A culture of cybersecurity in critical infrastructure must be established to shift mindsets toward designing systems with security in mind. An awareness of system vulnerabilities and designing and implementing standard security baselines will be a good start (Dimarucut, 2019).

Transportation

The transportation sector in the Philippines comprises a network of government agencies, private companies, transport operators, private vehicles, and the general public. It covers various modes of transportation, primarily including road, water, air, and rail. Administered by the Department of Public Works and Highways (DPWH), national roads are classified under primary (connecting two or more major cities), secondary (linking smaller cities and provincial capitals), and tertiary (other roads) (DPWH, 2019).

The Philippine transportation network is extensive. As of 2019, the country has a total of 33,018 km of national roads (DPWH, 2019). Railway transportation is mainly utilized within Metro Manila and consists of two commuter lines operated by the Philippine National Railways and three mass transit lines operated by the Light Rail Transit Authority and Metro Rail Transit Corporation. The country has a total of 70 airports, with 12 international airports in Clark, Davao, General Santos, Laoag, Mactan-Cebu, Manila, Kalibo, Puerto Princesa, Subic Bay, and Zamboanga.[42] There are two major airlines: Philippine Airlines (owned by PAL Holdings) and Cebu Pacific (owned by JG Summit Holdings).

The different modes of transport are under varied regulatory authorities. Railways are regulated by both the DOTr and the DPWH. Sea travel is covered by the Maritime Industry Authority or MARINA, an agency under the DOTr, but the ports are supervised by either the Philippine Ports Authority or the Cebu Ports Authority, which are also under the DOTr. Governance of national roads in the Philippines is under the jurisdiction of the DPWH. Air travel is regulated by the Civil Aviation Authority of the Philippines. Many of these agencies under the DOTr are independent and only attached to the department for policy purposes.

Cybersecurity Threats in Transportation

Cyber threats are present in three components of the transport infrastructure: transport vehicle, operating systems, and information/data systems.

Transport Objects/Vehicles. The primary component of transportation is the transport object or vehicle. Globally recognized regulations have been developed to mandate safety features that are built into vehicles. Automobiles, for example, have built-in warning systems to alert drivers of impending collisions. Cars also have airbags within the steering wheel, which will release during a crash. Airplanes use computer systems to activate emergency features including the release of oxygen masks when there is loss of cabin pressure. These examples illustrate how vehicle systems have been designed with passenger safety as the tantamount priority. In modern times, most of these functions have been digitized, relying on some degree of internal programming to operate.

Operating Systems. Operating systems primarily manage the flow of traffic, goods, and resources within a certain mode of transport. They include both the technology and physical infrastructure, such as air traffic controls, stoplights, tollways, seaport operators, and power grids, which coordinate the movement of transport assets. These systems ensure that transport vehicles are properly routed to avoid collisions and accidents. They also avert potential bottlenecks when traffic in roads and ports are not properly managed. With rapid technological advancements, most of these operations are being automated. Most toll booths, for instance, employ a radio-frequency identification system and process digital payments, replacing human operators. Artificial intelligence has also made self-driving automobiles a reality. Startups in the United States have begun servicing driverless buses as a means for companies to transport their products across states.

Information and Data Systems. The transportation sector is a unique repository of data given traces of information produced through the movement of individuals, goods, and services. Data collection is a major component of transportation susceptible to attacks.

Transport information systems are platforms used by transport operators to manage the logistics of servicing all passengers who avail of their services. These include online ticketing systems that are used for all modes of transportation. Airlines, for instance, collect

vital passenger information from their customers through online reservations. Information systems also include online apps of transport network vehicle services or ride-hailing services such as Grab or Uber. These applications contain records of passenger activity, including all locations to which they have traveled.

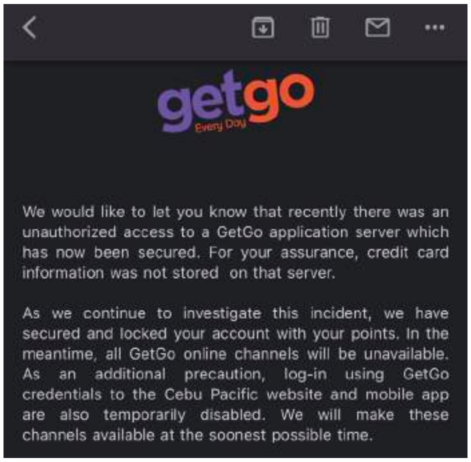
Cyber threats in transport operations include a variety of attacks that can compromise these components. The hacking of car systems has become increasingly prevalent, with modern vehicles containing a number of onboard computerized equipment, including an electronic control unit, Bluetooth connections, remote keyless entry, and other advanced digital features. Modern cars can also connect to the Internet through the use of internal servers. Hackers can introduce malware through these channels to disable important features or allow access to the car's functions by an external operator.

Another mode of attack comes from the interference of communications within transportation networks. Transportation systems often consist of subsystems that relay signals to one another. Routing and timing attacks can be mobilized to intercept these messages and modify their content, thereby incapacitating the system. In the case of air traffic control systems, the most common attacks are DDoS attacks where malware is used to lock operators out of their own systems (Haydari & Yilmaz, 2018).

Advanced traveler information systems are platforms that inform passengers of pertinent travel information including schedules, itineraries, travel times, and emergency information (Fok, 2013, p. 18). These systems contain internal data on transport providers and how their services are coordinated. Companies also use applications for individuals to register their personal details, such as biodata, credit card details, and addresses, to access information.

Mobile apps, such as maps, food deliveries, and ride-hailing services, also keep user information on an individual's locations. Ride-hailing platforms pose a special risk in that they contain the information of both the drivers, who often have to upload personal identification online, and their customers. Large businesses also rely on logistics providers to ship products within their supply chains. Often, logistics providers use information systems to track cargo and goods that use their fleet (Tam & Jones, 2018). Hackers can access and leak this information.

Transportation Cybersecurity Incidents



We would like to let you know that recently there was an unauthorized access to a GetGo application server which has now been secured. For your assurance, credit card information was not stored on that server.

As we continue to investigate this incident, we have secured and locked your account with your points. In the meantime, all GetGo online channels will be unavailable. As an additional precaution, log-in using GetGo credentials to the Cebu Pacific website and mobile app are also temporarily disabled. We will make these channels available at the soonest possible time.

Screenshot of the GetGo notification on unauthorized access on its server

In April 2019, Cebu Pacific Air reported a breach on their rewards platform GetGo (Rey, 2019). The attack was attributed to a local affiliate of the hacking group Lulzsec, which claimed responsibility for the breach. Cebu Pacific shut down its servers temporarily after the breach but assured the public that no credit card information was contained in the platform. The airline then reported the breach to the NPC, which conducted a thorough investigation of the incident. A similar data breach happened a year before with Cathay Pacific, which exposed sensitive information of 102,209 Philippine data subjects, including passport and credit card numbers. In this case, the NPC questioned why the airline reported the breach several months after the incident.

In November 2020, hackers were able to use an API[43] to set up a website that purported to be an official page of the Land Transportation Office (LTO). Thousands of users accessing the unauthorized LTO site were tricked into giving their information including their biodata and car registry details. The NPC's investigation revealed that 9,952 driver's license details and 19,406 motor vehicle data items, including make, plate number, engine number, chassis number, registration expiry, and owner, were leaked before the fake website was shut down (Samaniego, 2020).

The 2017 British Airway global outage, which caused the cancellation of more than 400 flights and stranded 75,000 passengers in one day, was not necessarily a cyberattack (Patrizio, 2017). But it did show the disaster that is possible when key systems are compromised. In this case, an unexpected power surge caused the total disruption of key IT systems, costing British Airway over EUR 100 million.

While transportation cybersecurity incidents in the Philippines have not yet led to such a significant level of economic damage, the magnitude of the potential consequences should be a cause of elevated concern to the transportation industry and the transport regulators.

Philippines Transportation and the Need for a Governance Framework

The documented cyberattacks on the transportation industry in the Philippines mainly centered on data breaches. Sensitive information was leaked both from the databases of private companies (Cebu Pacific and Philippine Airlines) and from public agencies (LTO). These relatively modest attacks were orchestrated by small syndicates as part of a fraudulent venture. Most incidents were isolated breaches that would not be replicated after thorough investigation. While the Cathay Pacific leak was more significant, the attack was perpetrated outside the country. The lack of larger attacks targeting systemic operations may be due to the relatively underdeveloped transportation infrastructure in the country. Compared to transportation in first world nations, transportation in the Philippines is modernized to a lesser degree. Smart automobiles fully connected to online systems have yet to penetrate the public market. The public transport infrastructure is mostly operated manually. Only recently have toll booths in two highway systems in Luzon utilized radio-frequency identification—and even then, the rollout of the technology was poorly implemented (Gonzales, 2020b).

Specific policies have already been floated to increase the cyber resiliency of critical sectors, such as transport, which rely on complex and overlapping information systems. One policy is the creation of sector CERTs, which are responsible for assessing and testing system vulnerabilities within the industry and enable agencies to uniformly comply with best cybersecurity practices, as prescribed by the DICT. Another recommendation would be for transport agencies to view cybersecurity through the lens of an interconnected ecosystem. Most digital equipment used by government agencies have been designed to be interoperable. A lot of data is also shared among various departments with overlapping functions. Given this reality, best practices must extend beyond an agency's internal operations toward the external transactions that they conduct. This includes a zero-tolerance approach to procurement where software equipment must be vetted for safety as a precondition for any purchases. External contractors who install these systems must also be given limited access to the rest of the agency's networks and only on a need-to-know basis.

Inevitably, growth in the Philippine economy will rapidly transform and digitalize transportation. Productive markets require mobility and a robust infrastructure for moving physical and human resources. As transportation systems digitalize, cybersecurity threats will also increase. With no precautions in place, attacks can become more sophisticated in targeting these increasingly automated systems, hence the need for a governance framework to manage these risks to transportation.

Future cyber threats in transportation may have implications not just on individual privacy but on public security as well. The transportation sector is a nexus where the movements of people and physical assets converge. An attack on a digital transport system can lead to increased accidents in the physical world. Moreover, paralyzing these systems can also paralyze economic activity altogether if the nation's mobility backbone is frozen. These harms have yet to materialize, and some may claim that they are merely speculative at this point. Yet, technological advancements will make these risks more possible, and the realities in other nations already point to these trends. The question for policymakers is not *whether* to confront these risks, but *when*.

Telecommunications and Internet

Given how extensively people use communications and the Internet in their daily lives, digital connectivity has become essential. In the early days, telecommunications operators maintained the public switched telephone network for making telephone calls. The ability to provide telephony services was a big boon in the development of human beings. It allowed people to freely communicate in real time outside the bounds of space. Today, technology is evolving to carry not just human voice in real time but even video, information, and all sorts of transactions that have become integral in people's lives.

Business, work, and school are increasingly being done online at home, a change that was especially palpable when the COVID-19 pandemic began. There are even demonstrable instances where stability of telecommunications and Internet services could spell life or death. Medical facilities and emergency care services, for example, rely on communications to address urgent medical needs.

It is thus no longer beyond imagination that any prolonged widespread loss of connectivity could cause significant injury to society. Many of today's critical services (e.g., financial clearing houses, SCADA networks, law enforcement, health, and other systems) depend on Internet services, most of which are provided by telecommunications networks. Disruption of telecommunications and Internet service could cause chaos by disrupting other critical sectors. For example, local financial service providers, such as banks and clearing houses, are dependent on electronic communications, the loss of which due to the interruption of telecommunications and broadband services could redound to losses not just for these providers but also for their customers. An entire country's economy could be compromised by such prolonged outage of telecommunications and Internet services.

Philippine Cybersecurity Response in Telecommunications

The National Cybersecurity Plan 2022 defines *critical information infrastructure* as systems and networks operated by critical infrastructure providers (i.e., telecommunications, water, power) that must be protected.[44] These CIIs play a vital role in the economy (DICT, 2017b). In Singapore, CII is defined as a computer or a computer system necessary for the continuous delivery of an essential service, and the loss or compromise of such would have a debilitating effect on the availability of the essential services (Singapore Cybersecurity Act, 2018). Availability is a key aspect of information security. Telecommunications clearly fits into these definitions of CII. Thus, telecommunications providers are expected to support and secure their infrastructure.

Through the years, several laws have been enacted that affect cybersecurity, mostly targeting cybercrime, and require the cooperation of telecommunications companies and ISPs.

- **RA 7925 or the Public Telecommunications Policy Act of 1995.** This law states that "[t]elecommunications is essential to the economic development, integrity and security of the Philippines." It obligates telecommunications providers to ensure quality, safety, reliability, security, compatibility, and interoperability of their services. The law clearly states that safety and security are key responsibilities of any service provider.
- **RA 9239 or the Optical Media Act of 2003.** Although the law does not explicitly mention telecommunications or the Internet, it regulates the use of optical media in the Philippines, supplementing the protection of intellectual property rights.
- **RA 8293 or the Intellectual Property Code of the Philippines of 1997.** Since a major mode of committing intellectual property infringement is via the Internet, service providers are inevitably intertwined with the enforcement of intellectual property laws.
- **RA 9775 or the Anti–Child Pornography Act of 2009.** This law makes ISPs responsible for responding to requests from law enforcement regarding violations of the law. While the law does not require ISPs to monitor users, it requires them to obtain and preserve evidence and to have filtering capabilities to remove content in violation of the law. This, together with RA 9262 or the Anti-Violence Against Women and Their Children Act of 2004, is key legislation protecting the vulnerable sectors and preventing the perpetration of cybercrimes, such as online sexual exploitation of children.

- **RA 10173 or the Data Privacy Act of 2012.** This law obligates personal information controllers, or entities that control the processing of personal information, to implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure. Telecommunications providers, who necessarily control the processing of personal information of their individual subscribers, are thus obligated to employ cybersecurity measures to protect the personal data in their custody.
- **RA 10175 or the Cybercrime Prevention Act of 2012.** This law requires service providers to help law enforcement entities gain capabilities to collect data in real time, preserve data as evidence, and prevent further execution of a crime.

As digital technologies are increasingly being used to commit various types of crimes, laws and regulations give more enforcement responsibility to service providers. In some cases, telcos and ISPs must, at the minimum, provide the capability to detect, record, and filter traffic. RA 9775 requires mass scanning against child pornography. Section 9 of RA 9775 requires ISPs to "install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered." This requires service providers to invest in these platforms' capability to collect information, including payload, and perform filtering, such as deep packet inspection or network probes. Thus, laws are putting the capability to perform mass surveillance and mass filtering in the hands of service providers, a development which, in turn, raises data privacy concerns.

Privacy Rights and Cybersecurity

> **A secure cybersecurity environment necessarily entails protection of privacy rights in general, secured by legal and technical safeguards.**

A secure cybersecurity environment necessarily entails protection of privacy rights in general, secured by legal and technical safeguards. Individuals enjoy a constitutional right to privacy, and entities have come to rely on an expectation of privacy when it comes to their private communications. The failure to provide or ensure privacy protections, whether from individual breaches to unauthorized mass surveillance of communications, should also be deemed as a cybersecurity failure.

Unauthorized wiretapping has long been a concern addressed by the legal system. As far back as 1965, the Philippines had already enacted RA 4200, which imposes criminal penalties on wiretapping activities that are not sanctioned by a court-issued warrant. Philippine courts have likewise adopted the "reasonable expectation of privacy" test, generally holding that any evidence resulting from the unauthorized interception of communications is inadmissible if the suspect had a reasonable expectation that such communications were private in character. The Bill of Rights of the Philippine Constitution itself explicitly protects as inviolable "the privacy of communication and correspondence," except upon lawful order of the court or when public safety or order requires otherwise, as prescribed by law.

The Cybercrime Prevention Act had originally included a provision that allowed law enforcement authorities to collect or record in real time traffic data on specific communications transmitted using a computer system, without need of a court warrant, upon a standard of due cause. The Supreme Court, however, declared such provision as unconstitutional in 2014, applying the test of reasonable expectation of privacy. According to the Supreme Court, when the right to privacy transcended the disclosure of private information and impinged on the right to live freely without surveillance and intrusion, the reasonable expectation of privacy should be measured from the general public's point of view—whether the infringement on privacy must be one that society was prepared to accept as objectively reasonable. In the end, the Supreme Court concluded that the broad sweep of the provision, unsupervised as the collection was by a judicial warrant, resulted in a violation of individuals' privacy. Since traffic data could allow analysts to determine a person's close associations, religious views, political affiliations, and even sexual preferences, such information was deemed as likely beyond what the public may expect to be disclosed; hence, the necessity of a warrant before such traffic data can be validly collected.

Thus, the general requirement is that interception or the recording of communications over telecommunications and ICT platforms requires a judicial warrant to be valid. Otherwise, those engaged in such wiretapping activities are liable to criminal penalties under the Anti-Wiretapping Act or the Cybercrime Prevention Act. The stringent enforcement of these laws would go a long way to deter unauthorized surveillance through telecommunications and digital platforms, whether undertaken by government or private sector actors.

Safe Harbor Protections for Telecommunications Platforms

A safe harbor clause is a legal provision to sidestep or eliminate legal or regulatory liability in certain situations, provided that certain conditions are met (U.S. Digital Millennium Copyright Act, 1998). Safe harbor clauses have become relevant in tackling the question of whether it is the responsibility of telecommunications service providers to ensure that no crime is committed using their networks.

In the United States, safe harbor clauses, particularly the U.S. Digital Millennium Copyright Act of 1998 (DMCA), have shielded American telecommunications platforms from liability arising from misuse committed by their customers. The DMCA defines four safe harbor provisions for determining copyright infringement: (1) providing transmission and network communications, (2) system caching, (3) information handled at the direction of users, and (4) information location tools. This substantially limits the liability of telecommunications providers in the case of copyright infringement complaints.

In the Philippines, Section 30 of the e-Commerce Act of 2000 provides that a service provider, or one who provides for or operates online services or network access, is exempt from civil or criminal liability arising from the publication, dissemination, or distribution of electronic data message or electronic document (thus encompassing online content), if the provider does not have actual knowledge that the material is unlawful or infringing, does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity, and does not directly commit any infringement or unlawful act. Section 30 has been recognized as a safe harbor provision that has shielded ISPs from liability arising from content posted or disseminated by its customers.

The presence of such safe harbor provisions could be cited by service providers in the Philippines as acquitting themselves of the responsibility to closely monitor the use of their systems by their users. However, subsequent laws such as the Anti–Child Pornography Act require ISPs to at least undertake the mass scanning of content to block or filter child pornography. Without these safe harbors, a telco or ISP would need to deploy deep packet inspection tools to analyze all traffic going in and out of their network to look for infringing materials. Yet, with the Anti–Child Pornography Act, at the very least, ISPs in the Philippines can be deemed as now having such surveillance capability, which could extend to content outside of child pornography.

Information Security in Telecommunications as a Two-Front War

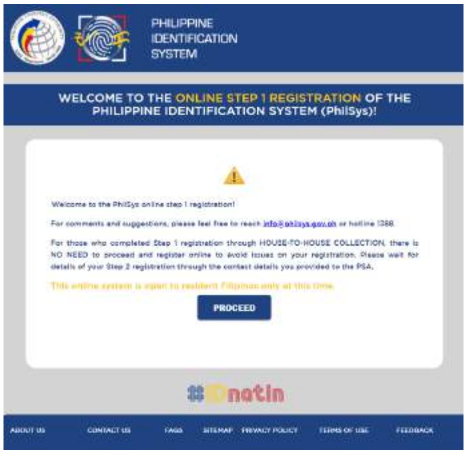
Information security for service providers has two sides. On one side, service providers must secure themselves as they are considered critical infrastructure. Information security risks could cause outages and damage to their infrastructure that is now deemed essential to the continuous operation of the state and general welfare of the nation. Yet, the current regulatory-legislative regime and the increasing dependence on digital infrastructure is increasing the responsibilities of service providers to enforce aspects involving information security. Hence, as technology is increasingly being used to commit crime, the role of the service provider in cooperating with law enforcement increases as well. The downside is that the capabilities of telcos to carry out mass surveillance and mass filtering can also be misused or exploited for illegal activity. In fact, the presence of these capabilities and information makes telcos a more attractive target for bad actors, unethical players, and entities wanting to perform espionage. Thus, it is important to protect telecommunications systems and the data that they collect as critical infrastructure and as espionage infrastructure.

There is a delicate balance between what is necessary to maintain a safe and democratic society and what is excessive. Technological capabilities can provide some of the most comprehensive powers of surveillance and censorship humanity has ever had. As technology progresses, these capabilities will continue to get more powerful. It is incumbent on any society that values freedom and democracy to resist the temptation to move toward more authoritarian uses of these technologies. Legislators must also take care when enacting new laws to ensure that democratic values and civil liberties are preserved and to prevent the excessive use of technologies.

National ID System

RA 11055 or the Philippine ID System (PhilSys) Act was enacted into law on August 6, 2018. The PhilSys aims to "provide a valid proof of identity for all citizens and resident aliens as a means of simplifying public and private transactions," as well as to "eliminate the need to present other forms of identification when transacting with the government and the private sector" (PhilSys Act, 2018, Sec. 3).

The PhilSys Act provides that every registered Filipino will be issued a Philippine identification card (PhilID) and that a unique PhilSys Number (PSN)[45] shall be assigned to each citizen or resident alien when they register with the PhilSys. The data collected will be recorded and stored in the PhilSys Registry (PhilSys Act, 2018, Sec. 6–7).



WELCOME TO THE ONLINE STEP 1 REGISTRATION OF THE PHILIPPINE IDENTIFICATION SYSTEM (PhilSys)!

Welcome to the PhilSys online step 1 registration!

For comments and suggestions, please feel free to reach info@philsys.gov.ph or hotline 1388.

For those who completed Step 1 registration through HOUSE-TO-HOUSE COLLECTION, there is NO NEED to proceed and register online to avoid issues on your registration. Please wait for details of your Step 2 registration through the contact details you provided to the PSA.

This online system is open to resident Filipinos only at this time.

Screenshot of PhilSys online registration

The COVID-19 outbreak and its resulting limitations on movement further delayed the full implementation of the PhilSys Act. President Duterte has lamented the inconveniences posed to the pandemic response by the nonimplementation of the PhilSys ID, which he said led to delays in the distribution of cash aid to citizens most affected by the enforced lockdowns (Esguerra, 2020).

However, the PhilSys ID has limited use. While the PhilSys ID would have made it easier to verify the identity of beneficiaries, it could not have been used as the sole basis for cash aid distribution sourced from the existing Social Amelioration Program.[46] The ID itself could not have supplied information on whether the cardholder was actually qualified for financial relief; that information independently came from the results of the census conducted in 2015 and was potentially outdated itself. As the Philippine Statistics Authority (PSA, 2020a) emphasized, the "processes beyond identity verification, such as authorization and identification of beneficiaries remain fully with the implementing agency/party."

Thus, there may be elevated expectations, and even elevated fears, concerning the implementation of the national ID system. Some of these fears may be mitigated by limitations on data collection and data security obligations imposed by the PhilSys Act. Yet, there is no question that the en masse collection of sensitive personal information of Filipino citizens and the storage of such information in a unique ID card that may be prone to loss or counterfeiting create heightened cybersecurity risks that should be addressed as the PhilSys ID is rolled out.

The Philippine Identification System Act

Table 3 shows the demographic data and biometric information collected from an individual under the PhilSys Act (PhilSys Act, 2018, Sec. 8).

A citizen registering in the PhilSys needs to present his/her birth certificate issued by the PSA and a valid government-issued identification document. A resident alien registering in the PhilSys needs to present their Alien Certificate of Registration or ACR ID. An applicant who does not possess any identifying document may be endorsed by someone of legal age and duly registered with the PhilSys (PhilSys Act, 2018, Sec. 10).

Table 4. Demographic Data and Biometric Information Collected under PhilSyS Act

Demographic Data	Biometric Information
1. Full Name 2. Sex 3. Date of Birth 4. Place of Birth 5. Blood type 6. Address 7. Filipino or resident alien 8. Marital status (optional) 9. Mobile number (optional) 10. Email address (optional)	1. Front facing photograph 2. Full set of fingerprints 3. Iris scan 4. If necessary, other identifiable features

Ideally, the PhilID/PSN will be sufficient proof of identification when transacting with the government and private establishments, subject to proper authentication (PhilSys Act, 2018, Sec. 12), thus doing away with the current practice of having to present at least two valid government IDs.

The PhilSys has data privacy mechanisms in place. Whenever a PhilSys ID holder transacts with an entity, their consent needs to be obtained first. As a safeguard, any demand from a cardholder to present their PhilID or divulge their PSN should be consistent with the foundational principles of transparency, legitimate purpose, and proportionality of RA 10173 or the Data Privacy Act. With the application of these principles, an ID holder needs to be informed of the nature of the information that may be shared upon authentication and what the information may be used for (PhilSys Act, 2018, Sec. 12).

Mandates of the Philippine Statistics Authority

The PSA is the lead implementing agency of the PhilSys Act. It is responsible for the overall planning, management, and administration of the PhilSys and is authorized to collaborate with various government agencies, including local governments and government-owned and controlled corporations, for the registration of individuals.

The PSA is the operator, manager, and personal information controller of the PhilSys. It is mandated to set up the PhilSys central system and database that will hold the registry data of individuals, as well as a network of registration subsystems in various national and local government agencies designated as registration centers and authentication subsystems in all relevant government agencies.

```
 1. Sep 15:53 .
 0. Sep 2015 ..
19. Sep 09:31 bin -> usr/bin
21. Sep 15:50 boot
19. Sep 09:32 dev
21. Sep 15:52 etc
30. Sep 2015 home
30. Sep 2015 lib -> usr/lib
34 23. Jul 10:01 lib64 -> usr/lib
96 1. Aug 22:45 lost+found
96 30. Sep 2015 mnt
16 21. Sep 15:52 opt
0 21. Sep 08:15 private -> /home/e
4096 12. Aug 15:37 proc
560 21. Sep 15:50 root
7 30. Sep 2015 run
4096 30. Sep 2015 sbin -> usr/bin
6 21. Sep 15:51 srv
300 21. Sep 15:45 sys
4096 12. Aug 15:39
4096 23. Jul 10:25 usr
var
```

Recognizing that the PSA does not have the expertise in ICT infrastructure, the law provides that the DICT may assist the PSA in implementing "reasonable and appropriate organizational, technical, and physical security measures to ensure that the information gathered for the PhilSys, including information stored in the PhilSys Registry, is protected from unauthorized access, use, disclosure, and against accidental or intentional loss, destruction, or damage." (PhilSys Act, 2018, Sec. 18). Additionally, the PSA is mandated to designate a data privacy officer for the PhilSys (Sec. 22).

If it has not done so yet, the PSA must address the development and/or acquisition of human resources with the right technical knowledge and expertise in information systems and network development and administration, as well as information systems security administration. The PSA must adopt minimum information security standards and develop and implement ICT policies and guidelines relevant to the development, management, operations, maintenance, and security of the PhilSys ICT infrastructure.

Implementation of the PhilSys Act and Challenges to Cybersecurity

Soon after the implementing rules and regulations of PhilSys were promulgated in October 2018, procurement of the technology and related services followed.[47] According to National Statistician and Civil Registrar Dennis Mapa, they wanted to "ensure that the processes are efficient, the systems are fully functional, and all information within the system [is] secure" (CNN Philippines, 2019).

In response to the president's lament about the absence of a national ID, the NEDA and its attached agency, the PSA, committed to fast-track the implementation of the PhilSys. The PSA targeted to register 5 million heads of poor families in the fourth quarter of 2020 (de Vera, 2020). While the target was not met,[48] registration eventually picked up. The PSA achieved its 2021 registration target, which totaled 50 million as of December 2021 (PSA, 2021b).

The existence of a national ID is always presented with security and privacy risks. It is critical to identify these vulnerabilities from the registration to the authentication process.

Privacy and Processing of Personal Data

The implementation of the PhilSys ID system will need to sufficiently address fears that an individual's right to privacy could be impaired. Past attempts at establishing a national ID system were met with opposition due to privacy concerns, which have been addressed over the years. Specifically, the issues include (1) access to personal confidential information without the owner's consent, (2) vagueness of the order and inadequacy of safeguards or penalties for any violation, and (3) lack of a compelling reason to legitimize the necessity of the order.

In 1998, the Supreme Court thwarted the attempt by President Fidel Ramos to institute a national ID system through Administrative Order No. 308. The Supreme Court agreed with the claims of former Senator Blas F. Ople, who argued in his petition that the policy infringed on the privacy of citizens. The Supreme Court held that the administrative order did not contain sufficient safeguards to the right of privacy, such as identifying who would control and access the data collected, under what circumstances, and for what purpose.

Several years later, President Macapagal-Arroyo issued Executive Order 420, which ordered government agencies to unify identification documents in the Unified Multipurpose ID (UMID). In response to a petition by Kilusang Mayo Uno, the Supreme Court allowed the UMID to move forward, noting that only 14 types of citizen data shall be collected, essentially the same data already collected by different government agencies issuing IDs. The Supreme Court also noted that the order provided safeguards that ensured protection of the confidentiality of data about citizens and that the order was legitimate, as it would result in efficiencies and lower costs for both government agencies and citizens. The UMID, however, is not just a simple identification card; it also provides access to services and benefits to the member government agencies. In the case of the Government Service Insurance System (GSIS), the UMID is also tied to a member's bank account.

Under the PhilSys Act, the data to be collected about citizens and resident aliens are limited to demographic data and biometric data, which are already collected by various government agencies.[49] Compared to the UMID, the PhilSys does not collect the identification numbers of members of Social Security System (SSS), GSIS, and other agencies or limit the card's uses for transactions with those agencies. The reverse, however, is true: The PSN will be seeded in other government agencies' systems. The limited collection of data in the PhilSys is a safeguard in itself.

The PhilSys Act provides several other security measures (PhilSys Act, 2018):

- Safeguards for data privacy and security, access controls, and change management (Sec. 7(b))
- Prevention against the proliferation of fraudulent or falsified identification cards (Sec. 7(c)(1))
- Consent of the PhilID/PSN holder prior to authentication (Sec. 12)
- Protection against unlawful disclosure of information/records (Sec. 17)
- Organizational, technical, and physical security measures (Sec. 18)

The PSA has been working closely with the NPC and the DICT regarding the architecture and process of the PhilSys infrastructure. Privacy-by-design principles have been adopted in the PhilSys, and the PSA also consults with the National Security Council on the architecture and process of the PhilSys (PSA, n.d.). This may raise concerns among civil society and human rights groups as it may lead to the slippery slope of surveillance.

PhilSys and the Data Privacy Act

The PhilSys Act meets the principles of transparency, legitimate purpose, and proportionality espoused by the Data Privacy Act[50] as it limits the number of personal information to be collected and processed by the PhilSys to be just enough to establish a registered user's identity. This is also consistent with the PhilID/PSN's declared purpose, which is to serve as sufficient proof of an individual's identity.

To protect data privacy rights, the PhilSys Act (2018) also enforces the following:

- Provides that consent be first secured from a registered individual before personal information, including record history, is disclosed to any third party or, if disclosed in compliance with a court order, that the registered individual be notified within 72 hours of the disclosure (Sec. 17 & 21)
- Allows any registered individual to access his/her personal information and record history (Sec. 17 & 21)
- Allows registered individuals to correct errors or omissions in their personal information recorded in the PhilSys Registry (Sec. 5(i)(3) & 4(i)(3))

The Data Privacy Act provides for a limited period of data retention (DPA, 2012, Sec. 11(e)). Since the authentication of PhilSys information returns a "yes/no" response, it is no longer necessary to retain personal information and authentication-related data. Absent a provision in the PhilSys Act providing for the aging and deletion of authentication entries in the record history, a registered individual may exercise their right to have the record history entries deleted as provided for in the Data Privacy Act.

Quick Response Code Vulnerability

The quick response (QR) code appearing on the PhilID, which stores the PSN and two-fingerprint information of a registered person, is a vulnerability, as it can simply be copied, tampered with, or used without authority.

The QR code stores data that is read by the authentication subsystem. This allows the encoding of the PSN and/or demographic information of a registered person and/or the capture of a registered person's biometric data. The authentication subsystem can be in online or offline mode.

Online, the authentication subsystem is connected to the PhilSys and is able to access the PhilSys Registry to perform real-time authentication. A "yes" response may be returned with the photograph of the registered person, which would then signify that the transaction could continue. A "no" response, on the other hand, would signal the requesting party not to proceed with the transaction.

Offline, the (sub)system is not connected to the PhilSys, but authentication can still be done on the basis of the PSN and two-fingerprint information stored in the QR code of the PhilID. If the PSN and fingerprint information retrieved by the authentication subsystem from the QR code match the registered person's, the system would signify that the transaction may proceed.

Vulnerabilities from Record History and Large Collection of Personal Information

The authentication records are effectively a historical record of a registered person's movement over time. This large collection of personal information can be a lucrative target for misuse.

The collection of entries of recorded events relating to a registered person's PhilID/PSN—registration, modification, issuance, cancellation, reissuance, and authentication—is known as the record history.

The process of authentication of the PhilID/PSN generates a record of the authentication request, which includes the date the request was made, the requesting entity, and the response of the PhilSys. The record is kept as part of the record history. The more frequently a registered individual uses their PhilID/PSN, the more authentication records are generated. The location of the requesting entity is not included in the collection, but the data collected may later be cross-referenced with other databases that will reveal the location of the requesting entity. Thus, a historical record of a registered person's movement can be generated over time.

The details of any authentication request are the most sensitive information that will be recorded when a PhilID/PSN is used. Thus, records should be stored or retained for a limited period only. A breach of the record history (it is not a matter of *if*, but *when*) may compromise the privacy of registered individuals, which may lead to the exposure of their activities and movements, exploitation of their identities, or worse, identity theft.

External Cyber Threats to PhilSys

> **No system or network is 100% secure from cybersecurity threats.**

No system or network is 100% secure from cybersecurity threats. Attackers may exploit known vulnerabilities of a system if these are left unpatched, if they discover new vulnerabilities and launch a zero-day attack, exploit misconfigured systems and appliances, try default passwords to gain entry, or launch social engineering attacks such as phishing.

The confidentiality, integrity, and availability of systems and data stored in such systems can be compromised at any time.

The PhilSys ID is no different. There are a number of *specific threats* that need to be monitored and prevented in order to keep the integrity and security of the national ID.

- **Counterfeiting of the PhilID.** Identification documents, like driver's licenses and passports, are known to be counterfeited. The PhilID, despite its security features, is not immune to falsification. A counterfeit copy of a PhilID may be used without authority for whatever purpose.
- **Illegal copy of the QR code.** The QR code printed on the PhilID can be copied, tampered with, or used without authority for whatever purpose.
- **Unauthorized use of a PSN.** An individual can use a PSN without authority for whatever purpose.
- **Abuse of PSN.** As provided by law, databases in government will be seeded with the PSN (PhilSys Act, 2018, Sec. 7(a)), which may then be used as the primary index key that will make data connections between systems easier. Once seeded, the PSN may be used to access the records of those registered in government agencies like the SSS and GSIS, which reflect employment records; the PhilHealth, which may hold health records; and the Bureau of Internal Revenue, which may reveal income. This, coupled with abuse of record history, can generate a good profile of an individual.
- **Abuse of record history.** An analysis of the registered person's record history would reveal his activities and movements. This may be combined with the information gathered from other government agencies using an individual's PSN. With data analytics, machine learning, artificial intelligence, and emergent quantum computing, personal information may be used, generally for profiling purposes. Worse, it may lead to the slippery slope of surveillance.
- **Unlawful disclosure.** The PhilSys Act provides that when public health or safety so requires, relevant information may be disclosed upon order of a competent court, with a 72-hour notification to the registered user (Sec. 17). This provision may be misused/abused by third parties, including law enforcement agencies, national security agencies, or the military, by building up a case with manufactured evidence to secure a court order to compel the PSA to disclose information about a registered individual.

The PhilSys may also fall prey to *common threats*. It may experience denial of service or *DoS/DDoS attack*, which can paralyze the whole PhilSys network and render data unavailable. *Ransomware* may be released and installed in the PhilSys, which would encrypt the contents of the database containing the personal information of registered citizens and resident aliens, thus making it unavailable. The PhilSys database may be *breached* anytime, and personal information of individuals may be pilfered, exposed, and/or sold in the cyber black market, which may result in the breach of confidentiality of personal information. PhilSys registered users may become victims of *identity theft* once bad actors get hold of personal information to commit *fraud*. The system could also become a victim of *human frailty*. An employee may be tempted to use personal information of an individual for *personal gain*. An employee may also be *bribed* or *harassed* into disclosing or altering personal information of citizens or resident aliens, resulting in the breach of confidentiality or integrity of personal information. Finally, an *untrained employee* may accidentally disregard security protocols and inadvertently disclose personal information of individuals.

Promoting the Information Security of PhilSys

The PSA, as the lead implementing agency, operator, manager, and personal information controller of the PhilSys, must assess its capacity to secure the PhilSys infrastructure, guided by the People-Process-Technology framework and create a comprehensive information security program. A framework is recommended below.

A. ***People.*** What knowledge, skills, and competencies would the PSA require to ensure a secure PhilSys infrastructure?

1. **Develop a Culture of Security Among Stakeholders**

   The PSA needs to develop and conduct awareness programs periodically and repeatedly, as technologies and practices evolve, even with the same audience. Awareness programs impart information on certain issues, in this case, matters relating to the PhilSys and PhilID/PSN, and how these can be secured from unauthorized access and use:

   a. ***For citizens and resident aliens:*** As part of the information campaign required under the PhilSys Act, the conduct of training on how citizens and resident aliens can protect their PhilID/PSN from counterfeiting, copying, and abuse.

   b. ***For employees of government agencies and private sector establishments:*** An awareness component on how to secure the PhilID/PSN while undergoing authentication and how individuals can secure their PhilID/PSN at all times.

   c. ***For employees of government agencies that will serve as PhilSys registration centers:*** An awareness component on how to secure the personal information of citizens and resident aliens who are undergoing registration.

   d. ***For workers at the PSA with particular focus on those assigned to operate and maintain the PhilSys:*** Periodic awareness sessions for employees on the importance of securing the PhilSys, including a component on information security, policies and guidelines, social engineering, and recognizing phishing attacks.

2. **Acquire or Develop Information Security Capability**

    a. The hiring of information security professionals and practitioners to manage the security of the PhilSys.

    b. Alternatively, the training and education of qualified employees in the field of information security.

B. ***Process.*** What policies and procedures would be needed that will guide security operations and management?

1. **Operational Policies, Procedures, and Guidelines**

    Policies provide guidance for employee action and behavior, such as what constitutes acceptable behavior. *Procedures*, on the other hand, provide a series of steps undertaken in the performance of certain activities. *Guidelines* provide the parameters that limit certain permissible actions. These are important tools for decision-making.

    Some of the security policy recommendations for PhilSys are as follows:

    a. Acceptable Use Policy stipulates allowable practices on the use and operations of an organization's ICT assets.

    b. Access Control Policy provides guidance for physical access to ICT assets and logical access to data stored in an organization's ICT systems. It provides guidance on what authorized employees can do with data, such as create, read, update, and delete.

    c. Change Management Policy provides guidance for making changes to the ICT infrastructure, systems, and procedures, including security services and operations. It allows methodical implementation to better manage the potential impact of change.

    d. Information Security Policy provides guidance for employees who use ICT assets.

    e. Incident Response Policy provides a structure for responding to incidents in order to limit the impact of incidents to business operations and ensure post-incident recovery at the shortest time possible.

f. Remote Access Policy provides for methods of remotely connecting to the organization's network. In the context of the PhilSys, it defines how the registration (sub)system and the authentication (sub)system will connect to the PhilSys.

2. Adopt Information Security Standards

Acting International Organization for Standardization (ISO) Secretary-General Kevin McKinley said, "Governments use standards as trusted solutions to complement regulation, and they give peace of mind to consumers who know they are not putting themselves or their families at risk" (Lazarte, 2016).

Below are information security standards from the ISO and the International Electrotechnical Commission (IEC) that may be adopted:

- ISO/IEC 27001 provides a structured approach to managing an organization's information security consistently and in a cost-effective manner.
- ISO/IEC 27002 provides guidance on applying security controls.
- ISO/IEC 22301 provides a framework for implementing a business continuity management system and minimizing business disruption and continued operations in the event of an incident.
- ISO/IEC 27031 is a framework on improving an organization's ICT readiness to ensure business continuity.
- ISO/IEC 27032 provides guidance on cybersecurity management to address cybersecurity risks.
- ISO/IEC 27701 provides a set of privacy-specific requirements and controls. This standard can help demonstrate compliance with the Data Privacy Act.

It is best that the PSA ensure that the PhilSys implementation design complies with listed standards to complement the security requirements of the Philippine Identification System Act. It would be highly desirable if the PSA itself certifies for ISO/IEC 27001 compliance.

3. Conduct Periodic Information Security Audit

Information security audit involves the inspection of an organization's information security posture—from policies and practices to implemented security controls. It can provide insight into areas that need rectification or improvement of defenses.

4. Conduct Periodic Vulnerability Assessment and Penetration Testing

Section 8 of DICT Circular No. 003 s. 2020 provides for the annual conduct of vulnerability assessment and penetration testing (VAPT) to ensure integrity and security of the government ICT systems (DICT, 2020). The VAPT may be conducted by the DICT's CERT-PH upon request by a government agency, or it may be conducted *motu propio* as determined by the Cybersecurity Bureau.

It is important to note that information security standards and audit requirements should not apply to just PhilSys itself, but also to systems that will connect to and use the data provided by PhilSys. These systems will be a common vector for data leakage if left unprotected. However, not all connecting systems have the same level of risk. The requirements should not create barriers for parties to participate in the proper use of the system. The PSA can implement a graduated system, where systems that need access to a few records can undergo a self-certification process, while systems that access a large number of records undergo full third-party certification.

C. ***Technology.*** What are the appropriate technologies required to secure the ICT infrastructure?

Upon proper assessment of the information security requirements, the PhilSys must identify and implement the appropriate technical solutions to protect various aspects of the PhilSys infrastructure:

a. Technical security solutions such as, but not limited to, firewalls, end-point security appliances, encryption, VPN, virus protection, and secure communication channels that may be used to connect the registration (sub)systems at registration centers and authentication (sub)systems at government agencies and private sector establishments.

b. Environment technology solutions such as, but not limited to, high-precision air-conditioning systems, dehumidifiers, uninterruptible power supplies, fire suppression systems, and others.

c. Physical access controls including electronic access controls with capability to log ingress and egress and closed-circuit television, among others.

d. Continuity solutions including backup PhilSys infrastructure (hot, warm, or cold sites)

D. ***Post-Audit and Post-Vulnerability Assessment and Penetration Testing.*** The policy, procedure, and skills gaps identified in the audit and the vulnerabilities uncovered following the VAPT must all be addressed in the most expeditious manner to ensure that the PhilSys is properly secured.

Security threats may not altogether be eliminated, and attacks on systems can happen any time. Security threats continue to evolve as technologies evolve, and they constantly grow in complexity, volume, velocity, variety, and value. Threats to the national ID, in particular, include counterfeiting of the ID, unauthorized use of the QR code and PSN, abuse of record history, and disclosure of personal information.

The PSA must take stock of the lessons learned by various other national ID systems. Among the biggest lessons are what data and how much data to put into the national ID database and the security concerns that come with it. It is clear that a federated approach to the national ID system allows better scaling of the ecosystem as opposed to a mechanism where all data is centralized in a single government database. The larger the pot, the more attractive the target. As the old adage goes, “Do not put all your eggs in one basket.” However, a federated approach also comes with its own risks, most of which are data privacy related. These concerns must be properly addressed by the government.

To address these threats, the PSA must assess its capacity to secure the PhilSys infrastructure and create a comprehensive information security program that will focus on people, process, and technology.

In the broader context, the government should develop a national cybersecurity capacity development program. Beyond this, the government should also encourage more industry–academe partnerships to address the dearth of cybersecurity professionals and practitioners, incentivize innovation, and promote research efforts in cybersecurity.

Automated Election System

Cybersecurity issues that affect the exercise of the ballot are among the most crucial that a nation could face. Free, fair, and credible elections lie at the heart of a democracy and empower citizens to freely choose the country’s leaders and representatives in government.

Elections in the Philippines have been held for over a hundred years. The country holds synchronized elections for national and local positions. Elections have historically been marred by allegations of irregularities, including fraud and cheating. A particularly notorious form of election fraud has come to be known as "*dagdag-bawas*" (a form of point padding or point shaving), where consolidated votes for a certain candidate are deducted and then added to the vote counts of favored candidates. Handwritten numerical figures as appearing in election returns have been manipulated in crude ways, such as altering the figure 3 into the figure 8 or the figure 1 into the figure 4.

The Philippine Commission on Elections (COMELEC) has sought to modernize the conduct of the elections. The use of automated election systems (AESs) has been seriously considered since the early 1990s. In 1997, the COMELEC was authorized under RA 8436 (as later amended by RA 9369) to implement an AES. However, it was only in 2010 that the first national and local elections using an automated system were finally held.

RA 8436 expressly embodies the goal of the use of an AES:

> [T]o encourage transparency, credibility, fairness and accuracy of elections… involv[ing] the use of an AES that will ensure the secrecy and sanctity of the ballot and all election, consolidation and transmission documents in order that the process shall be transparent and credible and that the results shall be fast, accurate and reflective of the genuine will of the people.

Despite the advantages offered by an AES, there remain several concerns arising from its actual implementation in 2010 that warrant resolution as they could affect public trust in the administration of the sacred electoral franchise.

Security Issues and Automated Elections

RA 8436, as amended, requires certain security measures to be put in place, designed to preserve the integrity of the ballot.

Ballot Security

RA 8436 requires certain safeguards implemented on the physical ballot itself to prevent the use of fakes. These safeguards include, but are not limited to, bar codes, holograms, color shifting ink, and microprinting.

The safeguards provided on each ballot used in the last four elections were (a) watermarks, (b) bar codes or QR codes, and (c) ultraviolet (UV) ink. The use of the barcode and QR code ensured uniqueness of each ballot and that the ballot may be used only at a specific precinct. The vote counting machines also included UV ink mark detection.

Digital Signature

Another security feature is the use of digital signatures in signing election returns and certificates of canvass. A digital signature is an electronic signature of a person[51] affixed on an electronic document. The election returns generated by the vote counting machines, and the certificates of canvass generated by canvassing and consolidation servers, are in themselves electronic documents. Digitally signing these documents ensures that the contents are protected against tampering and preserves the documents' integrity. The identity of the signers of the digitally signed election returns and certificates of canvass may independently be verified by the receiving parties.

Digital signing may be done with the use of a PKI, which is the procedure referred to in the definition of an electronic signature. The PNPKI (see discussion on e-government in the previous section) was established and is operated by the DICT. Members of the Electoral Boards and the Boards of Canvassers are functionally required to register with the PNPKI in order for them to use the facility for purposes of digitally signing the elections returns and certificates of canvass.

The digital signing requirement is provided in the following provisions of RA 8436:

- The last paragraph of Section 22 provides: "The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate."
- The last paragraph of Section 25 provides: "The certificates of canvass transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the proclamation of a winning candidate."

Some may argue that these provisions do not identify who shall digitally sign the electronically transmitted election returns and the electronically transmitted certificates of canvass. However, RA 8436 also effectively superseded the Omnibus Election Code or *Batas Pambansa Blg. 881*, which required that the election returns be signed by the members of the Board of Election Inspectors and that the certificates of canvass be signed by the members of the Board of Canvassers at all levels of canvassing of votes.

In recent automated elections, the mechanism implemented in the vote counting machines and the canvassing and consolidation servers was one that affixed "machine digital signatures" to the respective election returns and certificates of canvass. The respective members of the Boards of Election Inspectors and Boards of Canvassers would initiate machine digital signing following the entry or encoding of their respective passwords into the machine, prior to the printing and electronic transmission of the election returns and certificates of canvass.

Questions may be raised whether this mode of digital signing is consistent with legally recognized digital signatures under Philippine law. It should be noted, however, that digital signing is an act performed by a person, not by a machine.

Voter-Verified Paper Audit Trail

Among the minimum system capabilities required by law is the provision for voter-verified paper audit trail (VVPAT), popularized as "*resibo*," as well as a system of verification for voters to find out whether or not the machine registered their choice. However, neither of these required features was present in the precinct count optical scanner (PCOS) used in the 2010 and 2013 elections. The VVPAT was activated only in the 2016 elections, following the promulgation of a decision by the Supreme Court (*Bagumbayan-VNP v. COMELEC*, 2016), which ordered the COMELEC to enable the printing of the VVPAT. The delay in the implementation of these audit trail requirements, despite the explicit requirement of the law, is indicative of implementation issues of a law for the adoption of new technology.

Advanced Encryption Standard Network Security

Vote counting machines were deployed in close to a hundred thousand clustered precincts nationwide. Each vote counting machine is set to connect to its corresponding canvassing and consolidation server at the city or municipality, only after the election return has been prepared and the first few copies printed. This gave potential hackers a very short window of opportunity to interrupt or intercept the transmission of election results.

The canvassing and consolidation servers were open for a long period while waiting to receive transmissions from various sources (city/municipal level from the respective vote counting machines; provincial level from city/municipal servers; and national level from the provincial servers). While the window of opportunity left by the server is an obvious concern, there have been no reports of security incidents at any of the canvassing and consolidation servers at all levels of vote consolidation.

Data Security

The AES ensures that data at rest and in transit are protected against attacks to its integrity. Several of the system's features are designed to guarantee data security associated with the ballots and returns.

Encryption is a key means to ensure the integrity of the vote documents. Stored images of the ballots are encrypted. Even if hackers are successful in breaking into a vote counting machine, they would have a hard time breaking into each ballot. The election return is also encrypted prior to transmission so that even if hackers were able to intercept the transmission, it would require time to decrypt and manipulate the election return. Even if they are able to do so, hackers would have to find another opportunity to insert and transmit the manipulated election results.

The limited and controlled lines of transmission of data are also crucial to data security. In previous polls, election results from vote counting machines and canvassing and consolidation servers were transmitted through direct subscriber lines (DSL), general packet radio service (GPRS), satellite terminals known as very small aperture terminal (VSAT), and broadband global area network (BGAN). The election returns were transmitted to three destinations: the city or municipal canvassing and consolidation servers, the COMELEC's central server, and the transparency server. Copies of election returns received at the three destinations may be compared with each other to check if one or two copies have been compromised. This, however, has not been done in the past four elections where the AES was used.

Internal Threats

There were no reports of external interference in the AES network or its components. Insider threat, however, has not been completely ruled out. The possibility of insider threat has been demonstrated, for example, in 2010, when the supplier simply corrected the number of voters displayed at the COMELEC canvassing and consolidation for the Senate and party-list contests, as well at the canvassing and consolidation for the presidential and vice presidential contests in Congress. In 2016, the vendor's programmer, without first seeking proper authority, corrected the display of the names of candidates with the letter "ñ."

Local Source Code Review

The AES technology that is selected by the COMELEC is open for source code review. The last paragraph in Section 12 of RA 8436 particularly provides:

> Once an AES technology is selected for implementation, the Commission shall promptly make the source code of that technology available and open to any interested political party or groups which may conduct their own review thereof.

Notwithstanding the right of interested parties and groups to conduct source code review, the exercise of this prerogative has been hampered by limitations imposed by the developers of the system. The software used with the AES is proprietary, and the vendor exercises proprietary rights over the software. Even as RA 8436 does not expressly provide for restrictions on how the source code review is to be conducted, such limitations have in fact been in place, with the software developers invoking their proprietary rights. Such limitations include the following:

- Local source code review was done in a secluded location, and done only by approved reviewers.
- None of the reviewers can bring in any electronic device in the review location.
- While the reviewers had pens and notebooks with which they took notes, the notebooks had to be surrendered at the end of each review session.
- The conduct of the review was guided by a vendor representative, focused on preagreed sections of the source code.
- The version of the source code provided was a read-only copy.

These restrictions imposed on the conduct of source code review are arguably contrary to RA 8436. More fundamentally, they could even be infringing on the constitutional right of the people to information on matters of public concern.[52]

Accuracy of the Vote Count

The accuracy of the vote count is verified after the close of polls on the day of the election through the conduct of the random manual audit (RMA) as required by RA 8436, as amended. Table 4 shows the comparative details of the RMA results in the past four national and local elections.

Table 5. Comparative Details of RMA Results, 2010–2019 National and Local Elections

Election year	Number of legislative districts	Sample clustered precincts			Total number of sample registered voters who actually voted	Overall accuracy rate
		Target sample size	*Completed*	*Completion rate (%)*		
2010	229	1,145	1,046	91.4	540,942	99.5980
2013	234	234	212	90.6	111,251	99.9747
2016	238	715	687	96.1	330,813	99.9027
2019	246	715	711	99.4	403,839	99.9953

Note. Adapted from *2019 National and Local Elections Random Manual Audit*, by COMELEC, PSA, and LENTE, 2019 (https://comelec.gov.ph/php-tpls-attachments/2019NLE/Resolutions/mr190893_attachments.pdf).

Based on the benchmark accuracy rate of 99.995% of the vote counting machine set in the 2010 Request for Proposal, only the 2019 RMA outcome met the accuracy requirement.

A 99.995% accuracy rate translates to 1 vote mark erroneously read by the vote counting machine out of 20,000 vote marks. This means that in 2010, the PCOS erroneously read around 80 vote marks out of 20,000 vote marks. In 2013, around 5 vote marks were erroneously read. And in 2016, the machine erroneously read approximately 19 vote marks. The varying outcomes of the RMA may be attributed to humans assessing the vote marks. By simply looking at a vote mark, the human eye will easily fail to determine if the size of a vote mark passes the defined threshold or not.

Notable Issues Arising from the Conduct of Automated Philippine Elections

The same AES had been used in the national and local elections held in 2010, 2013, 2016, and 2019, each attended by issues and problems. Despite security measures put in place and the high level of vote count accuracy as reflected in the RMA results after each election, several issues remain a cause for concern.

Several issues emerged especially during the first conduct of automated elections in 2010:

- During the conduct of the final testing and sealing of the vote counting machine, errors in the counting of votes were detected. It turned out that the side of the ballot that had the local contests was redesigned from having single-spaced lines to double-spaced lines. The error caused the recall of all compact flash cards that contained the voting precinct configuration files nationwide.
- Among the security features then present in the ballot was the UV ink mark. However, on testing, the vote counting machine failed to detect the UV ink mark. The COMELEC resorted to disabling the UV ink mark detection feature and was forced to buy handheld UV ink mark readers for use by the Board of Election Inspectors. It was explained by the COMELEC that as ballot printing was quickly approaching the deadline, the ballots needed to be printed faster, resulting in the printing of the UV security feature at a lower ink density, which caused the UV ink detection to fail.
- Reports emerged after the election that the election returns had varying date and time stamps. According to its supplier, this was a result of batteries getting dislodged during transport of the vote counting machines.
- The PCOS had an external console port, which allowed a device like a PC or laptop to be connected to it. Accessing the machine internals did not require any password.
- The national canvassing and consolidation server at the COMELEC, which was used to aggregate the votes garnered by candidates for senator and party list displayed three times the number of registered voters.
- The national canvassing and consolidation server that was used by Congress (which is tasked by the Constitution to conduct the official canvass of votes for president and vice president) displayed five times the number of registered voters.
- As mentioned earlier, the AES used in 2010 failed to provide for a VVPAT and a system of verification for voters to find out whether or not the machine registered their choice. These features would not be provided for until 2016.

Since the initial AES in 2010, certain issues in the conduct of the 2013, 2016, and 2019 automated elections still emerged:

- The number of nontransmitted election returns increased from about 8,000 in 2010 to about 18,000 in 2013.
- In 2013, digital lines were found on ballot images in 11 out of 234 PCOS machines that were covered by the RMA, potentially impacting some 2,199,600 ballots.
- In 2016, observers at the transparency server operations saw that the names of candidates with the letter “ñ” were not being displayed properly. Hearing of the problem, a programmer of the software developer went ahead to apply corrections without first seeking proper authorization. Because of this, the election results

were delivered with conflicting hash codes through the transparency server. Consistent hash codes would have indicated that the election returns were free from tampering and had their integrity intact. The unauthorized action led some parties to allege vote manipulation.

- In 2019, the conveyance of election returns to election monitoring organizations, political parties, and media was halted within the first half hour of election returns transmission from the transparency server. This delay led to public concerns of vote manipulation to be raised anew. While efforts to show that none of the election returns were lost and that integrity was preserved, the cause of the glitch has never been completely explained.

Education

Following the COVID-19 pandemic, the Philippines has been forced to undertake policies that enable education technology as a means of implementing remote learning. With schools being potential hotspots of infection, the Philippine government decided to defer in-person classes until a vaccine becomes available (Al Jazeera, 2020). This has left students with remote learning, ideally from home, as the only option for continuing their education in the new normal, notwithstanding their households' capacity to access the Internet.

Public conversation has naturally focused on how remote learning will be implemented across all levels of education (Austria et al., 2020). Under K-12 alone, over 21 million students were enrolled for 2020–2021 (Montemayor, 2020). While centers of higher education tend to have more experience with remote learning compared to basic education institutions, many are still struggling with implementation due to Internet connectivity and other woes. According to the Commission on Higher Education, only 20% of state universities and colleges are equipped to conduct online classes (Gonzales, 2020a).

The DepEd, for its part, has committed to providing learning resources to all students using a mix of new and traditional media (Arcilla, 2020). But what has gotten much less attention from stakeholders are the potential security risks that arise from this new dependence on education technology.

EdTech in the New Normal

Education technology, also known as EdTech, refers to the use of technological tools, platforms, and services to enhance the education process for both teachers and students. EdTech has existed long before the pandemic began, in the form of comprehensive digital learning platforms, course management systems, massive open online courses (MOOCs), and even simple educational videos. In many cases, the goal of EdTech has been to complement—not replace—the classroom experience. This concept of combining online learning with classroom instruction is a growing branch of teaching called "blended learning."

Educational institutions have now been forced to rely on remote learning, entirely in some cases, in lieu of face-to-face classroom instruction. Some commentators have already expressed opinions about the merits of relying solely on EdTech from the perspectives of accessibility of online platforms and educational effectiveness. However, commonly overlooked issues involve the accessibility of devices and Internet connectivity, and the security and privacy risks that come with EdTech's surge to prominence in the new normal. Imagine all the millions of students and teachers suddenly needing to use technology full time. It is already difficult to get students, parents, and teachers to replace their display names or photos during online meetings, much more to require them to more comprehensively understand and practice information security.

Notably, the DepEd does not expect all students to use EdTech due to the poor state of connectivity in the country (Arcilla, 2020). Only 22% of public schools have access to the Internet, and DepEd, in preparation for remote learning, has allotted PHP 700 million to connect 7,000 public schools and coordinated with the DICT on the rollout of free Wi-Fi in public schools (Ramos, 2020b). In terms of household access, data from the 2019 National ICT Household Survey shows that although 95% of households have electricity, only 18% have access to the Internet at home, and 24% of households have communal computers (DICT, 2019).

The agency identified other modalities for home-based learning, including the use of printed self-learning modules, wherein printed collaterals and workbooks are distributed to students physically due to poor Internet connectivity and lack of access to appropriate devices, such as laptops and tablets. These are mostly available for schools in coastal areas, far-flung provinces, and communities without access to the Internet or electricity (DepEd, 2020). DepEd is also developing content for TV and radio, which, although may fall under the broad umbrella of EdTech, does not offer the same interactive experience as online learning. For the purpose of this report, EdTech refers to online solutions that use digital technologies.

Security Risks of EdTech

The privacy and security risks that come with giving young students access to resources on the Internet have existed for years. Online platforms often collect sensitive information from students, in addition to potentially sensitive data such as photos and videos. Improperly secured, this information could fall into the wrong hands and be used for identity theft and other similar crimes (Muncaster, 2018). For younger children who may be especially more trusting, this is a major concern as they can leave on cameras and microphones and may freely give information. In one instance, a cybercriminal group stole data from EdTech platforms and used children's information in various extortion schemes against the students' parents (Sullivan, 2019).

EdTech would be generally regulated by general laws on data protection, such as the European General Data Protection Regulation and the Philippine Data Privacy Act (Common Sense, 2019). This alone, however, is no assurance that any given platform will keep data secure. In 2019, for example, a study found that 80% of the most popular EdTech failed to meet adequate levels of privacy protection, despite the existence of regulations (Common Sense, 2019). The major reason is the *analog gap*. Content and information are secured in these centrally managed platforms, which are normally suitably protected. However, when a student or teacher produces or consumes content, it still has to be rendered on a screen, played back on speakers, or downloaded into a device. The digital information leaves the protection of the centrally managed and secured platforms. This content or information, converted from digital to analog in order to be perceived by humans, is what can be stolen or exploited.

Educational institutions must exercise due diligence to ensure that the EdTech they use follow best practices. Even then, there is always the risk of data breaches arising from attacks or negligence. They must also ensure that proper awareness campaigns are conducted regularly to ensure that students, parents, and teachers understand information security and privacy risks.

In September 2020, the Data Privacy Council Education Sector (DPCES), a group composed of private and public universities in the country, released a set of recommendations to ensure adequate data protection in the management and implementation of online learning (DPCES, 2020). Days before the scheduled start of classes in October, the NPC also issued Bulletin No. 16, providing a list of privacy guidelines for K-12 classes online learning for students, parents and guardians, teachers, and schools. The guidelines aim to protect personal information of the students as they engage in online learning (NPC, 2020b).

What makes EdTech particularly risky is that it is designed to be used by children and young people—a demographic that is unlikely to be fully aware of online dangers. Children are less likely to identify threats, such as compromised links, phishing attempts, and malware executables, leaving them vulnerable to attacks from malicious actors. Similarly, young people are less likely to discern what information they should or should not share online, which can be exploited by criminals in various schemes.

Beyond threats to data privacy, there are also other risks inherent to moving education online. Disruptions to online platforms due to DDoS or other attacks can leave students and teachers unable to access lectures, projects, and other activities (Fritchen, 2019). Attacks resulting in data loss, meanwhile, can have dire consequences, such as lost grades and schoolwork that can set back a school year (Fritchen, 2019). Also common are the attacks on university student portals, as what happened to Polytechnical University of the Philippines and Far Eastern University. Fortunately, no sensitive student information was compromised (Bernardo, 2020).

More students online means more user data to steal, making EdTech an even more attractive target for malicious actors. The attack surface in the education sector has become so big as to be potentially lucrative for malicious actors. Even platforms with a previously clean track record may have unexploited vulnerabilities, leaving them vulnerable to criminals taking advantage of the pandemic (Vijayan, 2020). Criminals are also using COVID-19-themed phishing attempts and other similar attacks, which impressionable young students may be particularly vulnerable to.

Mitigating Risks to EdTech

Shifting education online must be as secure and reliable as possible, both to minimize disruptions to learning and to keep students safe. Students, parents, and teachers need to be aware of the following threats that come with EdTech:

Identity Fraud. Cases of impersonation online is a problem for both teachers and students. For educators, issues can arise when they cannot verify whether it is actually the student doing classwork, submitting projects, and performing other requirements. In some cases, enterprising criminals even offer paid services to take online exams on behalf of students (Newton, 2015). Cases of impersonation can harm the legitimacy of diplomas and online certifications, affecting even students who have done everything by the book.

For students and parents, impersonation becomes a problem when teachers' accounts get taken over by malicious actors. In such cases, the person pretending to be a teacher may use the account to ask for students' pictures, personal information, and other sensitive data (Fritchen, 2019). Institutions should make sure that the EdTech they use has some form of verification process (such as having to show themselves on video) or, barring that, create a process of their own.

Fake Information. The sheer amount of false information online is a problem that affects the entire Internet, not just EdTech. However, as young students are less likely to discern between trustworthy and questionable sources of information, there is a real risk that students will fall prey to misinformation. EdTech relies on providing students access to the incredible amount of information on the Internet; however, educators need to teach students the proper skills to identify and avoid unverified, fake, or misleading information. It is generally safer for institutions to specify safe, authorized, and certified communications channels. It is best to avoid using public chat groups, forums, and platforms and instead use official institution email or other communications platforms, if available. For younger children, closed-loop and private systems are generally used, as no outside communications can come into the system. In some cases, moderating these channels adds a further degree of security. This prevents unauthorized and frequently unsavory messages from making it into the system.

Fake EdTech Platforms. As technology has evolved, diploma mills and other providers of fake credentials have moved their business online (Trines, 2017). Some diploma mills are now masquerading as legitimate institutions, especially for higher education. These websites pretend to be legitimate distance learning institutions, promising a quick and easy way to get a degree online (Trines, 2017). Potential victims are often enticed by supposedly "accelerated" programs that lead to a degree in a few weeks, or promises to convert work experience to academic credits. Students will have to take care to check that the institution they are signing up with is legitimate, accredited by LGUs, DepEd, or Commission on Higher

Education, and has a proven track record of producing legitimate graduates. As with anything procured in the open market, caveat emptor.

Phishing Attacks. These attacks use various social engineering tactics to convince teachers or students to send financial and other sensitive information. One education body has described phishing as the greatest security threat to EdTech, emphasizing the need to protect both students and teachers from this threat (Garry, 2019). As phishing relies on misdirection, a lack of awareness, or negligence, protecting against phishing means giving users the proper skills to detect such attacks. The fact that young students might not have the capacity to learn such skills yet adds another layer of difficulty. Educational institutions can help mitigate this risk by coursing all communications through a single, secure platform and teaching students that only communications through that platform are legitimate.

Practicing Safe Education Online

Successful education involves the cooperation of educators, students, and their parents; similarly, the task of securing EdTech is a group effort.

On the part of teachers and institutions, the first step is to follow good cybersecurity practices for all EdTech: ensuring all software is up to date, properly storing passwords and credentials, and keeping student information safe, among others. At the very least, online safety must be made part of developing education content and curriculum planning. As schools may opt to go with third-party EdTech, institutions should conduct due diligence on platforms used, to ensure that they follow good practices and have satisfactory privacy and security policies. Similarly, schools should conduct regular security audits of their EdTech to ensure the continued security of their platform of choice.

Organizations and institutions that have built and deployed these online platforms must have the proper information security tools and practices in place. Apart from identifying and protecting their assets and users, educational institutions must also have the proper people, processes, and technology to detect, respond, and recover from these threats.

In information security, people and organizations are only as strong as their weaknesses. All stakeholders must make an effort to increase information security awareness and improve cyber hygiene. No matter how secure the centrally managed platforms are, the users are always vectors of attack. With more frequent and various uses of digital platforms by more people, sectors that may not have been historically attractive to bad actors are now interesting.

For parents and students, it is important to learn what security features are available on the EdTech platform they are using and to follow the recommended guidelines to minimize exposure to risks online. Users should also limit the personal information they share, even on EdTech platforms. Avoiding suspicious emails and websites can also help prevent data theft and other potential attacks. Practicing good cyber hygiene is essential.

Pertinent laws to protect Filipinos from abuses in cyberspace are already in place, such as the Data Privacy Act and the Cybercrime Prevention Law. The NPC and private groups like the DPCES have also issued guidelines to ensure safe online learning and protect the personal information of students. In some countries, like the United States, specific laws for the protection of students have been enacted, such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and the K-12 Cybersecurity Act.

Government bodies also have an opportunity to ensure the security of EdTech. Ensuring that all schools and EdTech providers follow the applicable privacy laws is an important step to securing students' data. Educational institutions, and the DepEd in particular, may explore partnerships with industries and private sector companies who are engaged in the business of security and have effectively protected their data, to harness expertise in addressing vulnerabilities in privacy and security risks in online learning.

A forum for educators to share their practices and policies would be very helpful, particularly for those institutions with scarce resources. Publishing a list of best practices for schools to abide by is another way to enhance security, similar to those published by the U.S. Department of Education's Office of Educational Technology. An assistance center may also be set up, as well as protocols for the timely reporting and response to privacy concerns or incidents in online learning.

Finally, continuous information and education campaigns will be vital. DepEd has made strides on this and partnered with Globe, Plan International Philippines, and UNICEF SaferKidsPH to design e-modules on proper online behavior (Malipot, 2020).

While security online will always be a question of risks and probabilities, embracing EdTech is crucial in facilitating the education of an entire generation now faced with a pandemic and going forward in a post-COVID-19 world. The key is to ensure that technology allows learning to continue in a safe and effective manner in the new digital normal.

Working from Home

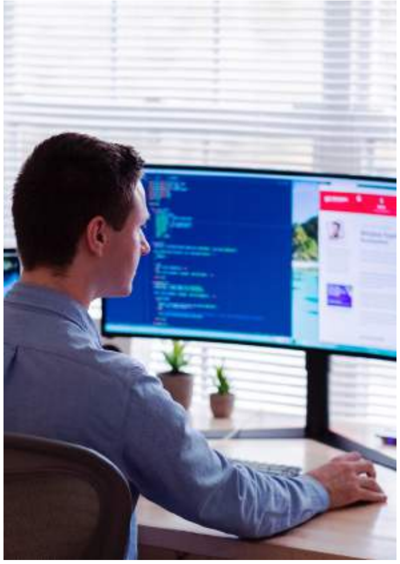
Even before the disruption of the COVID-19 pandemic, there has been increasing recognition that the future of the Philippine workplace will partly be in homes. Challenges such as the traffic situation in Metro Manila and unnecessary overhead costs have made telecommuting a more enticing alternative for both business owners and employees. The emergence of work-from-home (WFH) arrangements led the Philippine Congress in 2018 to enact RA 11165, also known as the Telecommuting Act. This law recognizes the practice of telecommuting, or work arrangements that allow private sector employees to work from an alternative workplace with the use of telecommunication and/or computer technologies. Thus, the same workplace entitlements and protections were accorded to employees who performed their tasks under WFH arrangements.

The COVID-19 pandemic has put unprecedented stress on the country's labor force, as quarantine measures have limited movement and forced many businesses to temporarily close. WFH leverages digital technology to move business operations online, with employees clocking in virtually and businesses providing access to their internal networks using virtual private networks or similar solutions over the public Internet.

The Philippines' Department of Labor and Employment puts the number of establishments implementing WFH at 2,662 as of April 24, 2020, equivalent to 70,649 workers (Jaymalin, 2020). This number seems severely understated, given that many the country's knowledge workers in the business process outsourcing (BPO), IT, and telecommunications space are currently under WFH arrangements (Campos, 2020). As quarantine measures persist, these numbers have likely gone up, and so has the number of networks that are potentially at risk of cyberattacks.

What is at Stake with WFH

Despite prior measures, such as the enactment of the Telecommuting Act, it was evident that not even technology-dependent businesses were prepared for the sudden en masse transition of their workforce to home office arrangements. Even BPO firms were deemed "largely unprepared for a total work-from-home model and had to overcome challenges related to internet access, equipment transfers, and clearance requirements from clients" (Salazar, 2020).



WFH arrangements also present new or evolved security threats to a business's cyber assets. In order for WFH to be possible, organizations have to release information and provide access to systems over public networks. This creates the added risk of these systems and information possibly falling into the wrong hands. The consequences of such leakage to finances and business reputation could be significant.

Cyber Risks of WFH

Cloud Services and Virtual Private Networks

Working remotely entails connecting an internal network to the public Internet in order to provide access to business services and resources, opening the proverbial Pandora's box. Two of the most common ways to work from home are (1) using a cloud service provider to host the organization's network or (2) facilitating access to the internal network from the Internet using a VPN. In short, either "put what we have outside" or "let people in."

A cloud service provider is an entity that provides cloud-based platform, infrastructure, application, or storage services, to other organizations (Microsoft, n.d.).[53] It hosts other entities' data and services on their servers, then users send their login credentials to the cloud provider's servers, which then grant access to an organization's resources. This is what it means to put what we have outside.

A VPN is "an encrypted connection over the Internet from a device to a network" (Cisco, n.d.). Once a user logs in to their organization's VPN client, the VPN creates an encrypted tunnel through which all traffic to and from the business's internal network is coursed. This is letting people in.

Regardless of what method is used to provide remote access, the integrity of all parts of the network is paramount to ensuring the security of sensitive business data and services. Modern cryptography and virtualization technology have made both options quite secure and accessible. It is good practice for one to go as far as to apply both technologies. Unfortunately, WFH makes such practice much more difficult to implement due to the complexity of managing the security for tens, hundreds, or even thousands of employees remotely. Given time, most organizations can roll this out. But with the pandemic and mobility restrictions, many organizations only had a few days to make it work.

Businesses can ensure that only authorized individuals get access to digital resources and services through what are known as identity and access management (IAM) systems. The implicit assumption of IAM is that anyone with the correct login credentials—in most cases, a username and password—is who they say they are, and therefore have authorized access to the network. Under WFH conditions, however, there is an increased risk of credentials leaking due to compromised devices, social engineering attacks, dumpster diving, or a combination of these. These problems can be especially pronounced for organizations that previously did not implement remote work and only did so out of necessity due to lockdown conditions.

WFH and Compromised Devices

Regardless of how remote access is facilitated, security relies on the integrity of all devices connected to the network. In an office environment, this is usually done through strict IT controls, which include managed devices, network filters, and strict access policies for IT assets.

Under WFH, however, IT management and support of employee devices must be done remotely. For some organizations, even managing on-site network and device infrastructure has become harder due to the lockdown limiting the movement of employees.

While it is not impossible to continue managing device security—tasks such as installing software or applying critical updates can be done remotely, for example—it is undoubtedly much harder to do so on the massive scale necessary for WFH. WFH has exponentially increased the already steep learning curve of managing security from afar, especially for businesses without prior experience with remote work.

Further complicating the picture are the practical difficulties inherent of BYOD policies, where employees are allowed to use their personal devices to access the organization's network and other IT resources, rather than companies issuing dedicated work devices to employees (Citrix, n.d.). Organizations that did not, or could not, issue dedicated devices—such as phones, tablets, and personal computers—to employees before the lockdown now have no choice but to implement BYOD policies.

Unfortunately, personal devices are often lacking in security due to a combination of poor security awareness and risky online behavior from users. Personal computers often have outdated antivirus software and may also be used to download illicit and often malware-ridden content from the Internet, such as pirated software. Smartphones may contain questionable apps or be used to visit compromised websites.

Organizations with existing BYOD policies before the pandemic are better prepared, both in terms of securing users' personal devices and instilling secure behavior among employees. Those who have been forced to adopt BYOD due to the pandemic now have to contend with the possibility of thousands of unsecured devices being used to access organization resources and data, opening themselves to a potential data breach.

Businesses may, therefore, be exposing themselves by allowing access to their networks from unsecure devices. Should device vulnerabilities lead to IAM credentials falling into the wrong hands, cybercriminals can gain access to sensitive business information, disrupt operations, or in a worst-case scenario, take over an entire system.

Even if end users' devices are safe, however, the security of WFH cannot be assured, as there are other opportunities for IAM credentials to leak.

Any remote device accessing business resources will have to go through a network of networks—the Internet. In practice, this means layers of network equipment and infrastructure that are beyond the control of an organization. Vulnerabilities, such as compromised routers (Seals, 2020), fake network switches (Jaffee, 2020), and network equipment with backdoors (Cimpanu, 2020b) are all possible avenues where IAM credentials can be intercepted and stolen. This is why the appropriate information security technologies must be applied to reduce the risks.

While service providers generally work to ensure the security of their networks, and although practices such as encrypting traffic through a VPN can mitigate the risk, organizations need to be aware that WFH compounds threats that did not exist or were minimal when the majority of employees worked on-premises. It is generally best practice for employees and organizations to secure their own systems and connections, regardless of the work arrangement.

Third-Party Provider Security

With many organizations forced to adopt WFH in order to survive, businesses might have felt pressure to obtain the services of a cloud service or VPN provider as quickly as possible. Unfortunately, not exercising due diligence with this decision could be massively harmful to an organization's security.

Numerous examples exist of disreputable service providers compromising their clients' security, leading to data leaks or even interrupting operations. In one case, VPNs that promised not to log their customers' activities—an important security feature for business and individual users alike—not only logged them but also leaked the data through poor security practices (Kan, 2020). Similarly, cloud providers that fail to adequately secure user credentials can lead to attackers gaining access to business data and services (Cimpanu, 2020a).

Even well-meaning and respectable service providers can be subject to cyberattacks. In the case of Dave, a U.S.-based banking app, a large amount of data was leaked due to an issue with one of their identity providers (Schwartz, 2020). Due diligence is necessary, but appropriate controls must also be put in place to limit the damage of exploits.

All these emphasize the importance of choosing the right provider for remote operations. Unfortunately, security considerations dictate that only providers are privy to the full details of a VPN or cloud service's operations. Without this firsthand information, businesses have no choice but to take providers' commitments at face value. Organizations should, therefore, look at other measures of a provider's trustworthiness, such as corporate ownership and market position, to hedge against the possibility of an unsecure provider.

Social Engineering Attacks

A 2020 survey by Malwarebytes revealed that almost 45% of employees have not undergone cybersecurity training that was focused on the potential threats of WFH, making the employees the weakest link.[54]

Social engineering attacks have been a significant cybersecurity risk even before the onset of the pandemic. These attacks, which involve tricking employees into divulging credentials or providing access to unauthorized users, represent a significant proportion of data loss or theft cases (Pilette, 2021; Draper, 2020). In other cases, attackers trick employees into transferring money to them—a larger scale, and likely a more profitable scam, relative to the common Nigerian prince scam (Australian Competition and Consumer Commission, 2020). With many employees working from home, cybercriminals are taking advantage of unfamiliar working conditions and pandemic-related anxieties to conduct attacks on employees and organizations.

Some attackers are using COVID-19-themed lures to bait individuals into giving up personal information in widespread phishing schemes (Trend Micro, 2020). BEC attacks are also on the rise, preying on employees who are just getting used to conducting all communications and activities over the Internet (Trend Micro, 2020). Compared to general phishing attacks, BECs are much more sophisticated and harmful. Attackers spoof the business email address of a trusted, usually a more senior organization member (such as a CEO) to gain the trust of one or more targeted employees. These employees are then tricked into making fraudulent wire transfers to overseas accounts, often leaving businesses with little recourse to get back their stolen money.

What is clear is that employees represent a serious point of vulnerability to organizations that are just getting used to WFH. Even the most secure systems can fall prey to an erring employee through an act as simple as sending their account password to an attacker pretending to be a colleague. In more innocuous cases, this may result in a relatively minor annoyance—such as a Zoom bombing after an employee inadvertently shares a meeting link publicly (O'Flaherty, 2020). In others, however, social engineering attacks on employees can lead to serious financial and legal ramifications on businesses.

Securing WFH

There are several recognized best practices that individuals and enterprises can adopt to enhance cybersecurity within WFH arrangements.

Secure Connectivity. Secure Internet connectivity is crucial in enabling employees to continue to gain access to company assets and resources. VPNs and software-defined wide-area networks have become essential tools in providing the requisite security for these connections.

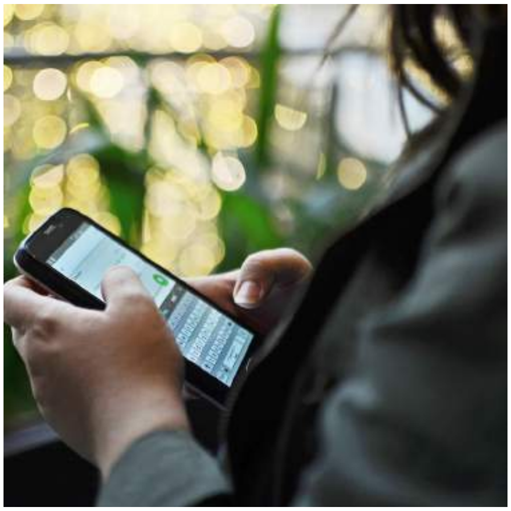
Secure Access to Systems and Applications. Work resources must be made accessible in a safe and secure manner. For example, developers must get access to source code, call center agents must get access to customer information, and many more. These systems can be deployed in the cloud. Whether private or public, cloud access provides the infrastructure to host these applications and make them accessible to remote users. Gone are the days of having applications installed solely in one's workstation. Virtualization technology provides applications with multiple options on where to reside, with many of them providing good accessibility. This can also apply to entire desktops and applications with technology, such as virtual desktop infrastructure (VDI) and application virtualization (AV). VDI allows access to one's entire workstation, while AV allows an application to be virtualized in order to be accessed anytime, anywhere, on any device. This portability is necessary when implementing WFH.

Managing One's Identity. To ensure that only authorized individuals get access to digital work resources and services, businesses implement IAM, which involves assigning identities to all users and managing the privileges they have in the business network (Strom, 2018). In this way, for example, only management can gain access to top-level financial information, and employees only access data and services relevant to their work. IAM is critical to ensuring both the internal (involving organization members) and external (involving outside actors) security of the network.

Failure to properly implement IAM can lead to loss of business data and disruption to operations and processes. Particularly when financial or customer data is involved, IAM failure can also lead to legal liabilities for the organization, as provided by the Data Privacy Act and other pertinent regulations.

Ensuring that IAM systems are secure is, therefore, critical to an organization's overall cybersecurity posture. When implemented for a local network, IAM systems can be secured by storing all user credentials—usernames, passwords, and anything else used to gain access to the system—in a centralized, secure, authoritative source (Microsoft, 2021). This makes it more difficult for outside actors to steal credentials that can be used to gain network access. The rise of WFH, however, complicates the security of IAM by introducing new points of vulnerability in the system.

Securing One's Access Devices. A major cause of stolen information is lost or stolen devices (WHOA.com, n.d.). This has become a larger risk as more people engage in WFH. Proper controls must be put in place to ensure that information is secure on these devices. Common tools in this space are mobile device management, which allows organizations to remotely wipe or remove data on lost devices and enforce information security policy; full disk encryption, which encrypts information in devices to prevent unauthorized use; and data loss prevention, which enforces policies to ensure that privacy-sensitive information is not being leaked. Protecting the end point has become a key aspect in a secure WFH environment.



Managing the End-to-End Security Life Cycle. Information security is not only about putting the right tools and technology in place. It is also about planning and responding to threats properly. An end-to-end life cycle approach must be taken when looking at information security.

The U.S. NIST information security life cycle specifies five key functions that must always be present: identify, protect, detect, respond, and recover (NIST, 2018a). An organization must be able to *identify* threats and see its risk profile in the context of its existing threat landscape to better prepare and implement the proper controls. It must also protect key assets and resources from these threats. This is the aspect that people focus mostly on when looking at information security tooling. An entity should also be able to detect when its controls do not work out and it is exploited. Even the best of preparations cannot prevent all forms of cyberattack. This is why an organization must be ready to *respond* if these attacks do happen in order to mitigate potential damages. Ultimately, it should be able to *recover* from security incidents. Any organization that is strongly dependent on IT and has a risk profile must strengthen all five functions of information security.

To ensure organizations mitigate the cybersecurity risks of WFH, businesses should create remote work policies that all employees should follow. WFH policies should, at the minimum, encompass the following areas:

Adopt an information security plan aligned with the five functions. Organizations should set strict standards for what devices can be used to access the business's data and resources. For business-issued devices, this can include limits on what hardware can be used with devices to minimize the risk of malware getting onto the system. Otherwise, businesses should include a BYOD component in their WFH policies that cover aspects such as mandatory antivirus software and limits on what other software can be installed on the system. In both cases, all software should be kept up to date to ensure the security of the devices.

To minimize the possibility of man-in-the-middle attacks, WFH device policies should also ensure that the devices are only used on trusted networks. This means avoiding the use of public networks in coffee shops and similar spaces, where the likelihood of someone snooping on network traffic is much higher compared to one's home.

Attacks are bound to happen, and organizations need to be ready to respond to possible breaches or some other compromise of their data and resources. Emergency response plans should be updated to reflect the shift to WFH, taking into account that employees might not have immediate access to a supervisor or an IT department. Setting up a dedicated hotline or point person that will be available 24/7 to respond to any emergencies should be considered. In the same vein, the plans should reflect the increased risk that comes with a sudden large-scale shift to WFH.

Review initiatives with an information security lens. The pandemic is a good opportunity, especially for companies who will be using cloud or VPN providers for the first time, to review the security and related policies of any third-party providers used by the business. This involves looking into not just the declared terms and conditions of the network but also any cybersecurity industry developments that might affect a provider's reputation. At a minimum, business stakeholders must be made aware of what is at risk should their provider be compromised.

Cyber hygiene initiatives. Promoting information security awareness and instilling a culture of cybersecurity are difficult tasks at the best of times, and pandemic conditions pose an additional challenge to teaching employees the best practices to observe online. Nonetheless, consistent reminders are necessary to give personnel the best chance at keeping their organizations' digital assets safe on their own. Employees should at least be taught how to distinguish between legitimate communications and possible phishing attempts, ways to securely store account credentials and other sensitive information, and how to avoid possible sources of malware, such as pornography and other illicit sites.

For organizations that do not yet have plans in place, the shift to WFH presents a good opportunity to develop responses to any possible eventuality.

WFH is a strategy for remaining productive in these most challenging times. Organizations should exercise caution to ensure that WFH remains a boon and not a bane to their business. Mastering the ability to harness a distributed workforce that can function at any place at any time with any device is powerful, with or without a pandemic.

Benchmarking the Philippines vs. Other Countries

How does the Philippines fare in cybersecurity compared to other countries? This section presents the ranking of the Philippines vis-à-vis ASEAN members and other Asia Pacific countries using the Global Cybersecurity Index (GCI) and the National Cybersecurity Index (NCSI), which measure the capacity and institutional readiness of national governments to respond to evolving cybersecurity threats.

Global Cybersecurity Index

The GCI measures the commitment of countries to cybersecurity at a global level. A total of 25 indicators are measured in the GCI: (1) legal measures, (2) technical measures, (3) organizational measures, (4) capacity building, and (5) cooperation. Indicator scores are not provided in the report (International Telecommunication Union, 2019).

The Philippines scored 0.643 and ranked 58th among 193 International Telecommunication Union member states. Among the 10 ASEAN member countries, the Philippines ranked 6th. Compared with other countries covered in this review, the Philippines ranked 13th.

Table 6. Global Cybersecurity Index Score and Ranking of Select Countries

Country	Score	Global rank	ASEAN rank	Rank in this review
United States of America	0.962	1		1
Singapore	0.898	6	1	2
Malaysia	0.893	8	2	3
Canada	0.892	9		4
Australia	0.890	10		5
Japan	0.880	14		6
South Korea	0.873	15		7

Table 6. Continued

China	0.828	27		8
Thailand	0.796	35	3	9
New Zealand	0.789	36		10
Indonesia	0.776	41	4	11
Vietnam	0.693	50	5	12
Philippines	0.643	58	6	13
Brunei Darussalam	0.624	64	7	14
Lao PDR	0.195	120	8	15
Myanmar	0.172	128	9	16
Cambodia	0.161	132	10	17

National Cybersecurity Index

The NCSI is a global index that measures “the preparedness of countries to prevent cyber threats and manage cyber incidents.” It is also “a database with publicly available evidence materials and a tool for national cybersecurity capacity building” (e-Governance Academy Foundation, 2020).

A total of 46 indicators are measured in the NCSI, spread across four categories: (1) legislation in force, (2) established units, (3) cooperation formats, and (4) outcomes/products.

The Philippines scored 63.64 and ranked 36th among 160 countries that responded to the NCSI. Among the 10 ASEAN member countries that responded, the Philippines ranked 4th. Compared with other countries covered in this review and that responded to the NCSI, the Philippines ranked 8th.

For baseline cybersecurity indicators, the Philippines scored high in terms of protection of personal data, with the presence of the Data Privacy Act. In terms of incident and crisis management, the Philippines also scored high in the fight against cybercrime because of the presence of a law on cybercrime prevention. It scored lowest in terms of protection of essential services, due to the absence of legislation that identifies essential services and require operators to manage cyber/ICT risks (e-Governance Academy Foundation, 2020).

Table 7. National Cybersecurity Index Score and Ranking of Select Countries

Country	Score	Global rank	ASEAN rank	Rank in this review
Malaysia	79.22	16	1	1
United States of America	79.22	17		2
Singapore	71.43	26	2	3
South Korea	68.63	29		4
Canada	66.23	30		5
Australia	66.23	31		6
Thailand	64.94	32	3	7
Philippines	63.64	36	4	8
Japan	63.64	37		9
New Zealand	55.84	49		10
Brunei Darussalam	41.56	76	5	11
Indonesia	38.96	80	6	12
Vietnam	36.36	83	7	13
China	35.06	87		14
Lao PDR	18.18	117	8	15
Cambodia	15.58	123	9	16
Myanmar	10.39	140	10	17

Endnotes

1 For a definition and list of critical infrastructure by select countries, see European Commission (Migration and Home Affairs, n.d.), Cybersecurity and Infrastructure Security Agency (2020), Department of Home Affairs (2020b), National Cyber Security Agency (2022), and Cyber Security Agency (2022).

2 Cybersecurity focuses on the protection of the CII or the computer systems and ICT networks of critical infrastructure. However, computers and ICTs are now integrated more and more into the design and functions of physical infrastructure. Over a decade ago, this was described by the U.S. Strategic Foresight Initiative (2011) as "cyber-physical systems." Examples are smart grid technologies, automated traffic control systems, and smart water meters.

3 The U.S. Patriot Act (2001) defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Cybersecurity and Infrastructure Security Agency offers an expanded definition to include "networks" (Cybersecurity and Infrastructure Security Agency, 2020).

4 The European Union defines "critical infrastructure" as an asset, system or part thereof located in member states, that is essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being of people, and the disruption and destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions (European Union, 2008). For an indicative list of critical infrastructure sectors identified by EU members, see Commission of the European Communities (2005).

5 For Australia, critical infrastructure "provides services that are essential for everyday life" such that its "disruption could have serious implications for business, governments, and the community, impacting supply security and service continuity" (Department of Home Affairs, 2020b). A comprehensive list of critical information sectors can be found in Cyber and Infrastructure Security Centre (2021).

6 Singapore's Cybersecurity Act (Cyber Security Agency, 2022) defines "critical information infrastructure" as "a computer or a computer system located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore."

7 Malaysia defines "critical national information infrastructure" as "those assets (real and virtual), systems, and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on national economic strength, national image, national defense and security, government capabilities to function, and public health and safety" (National Cyber Security Agency, 2022).

8 "Government" may include government facilities and functions, armed forces, civil administration services, and postal and courier services.

9 "Energy" may include electricity generation, transmission, and supply; oil production, refining, treating, storage, and transmission by pipelines; gas production, refining, treatment, storage, and transmission by pipelines, as well as liquefied natural gas terminals.

10 "Water" may include the provision of drinking water, control of water quality, and sewerage and wastewater systems.

11 "Communications," for the purpose of this report, may include telecommunications as well as information and communications technology (ICT) comprising hardware, software, IT systems and services, and the Internet. It may also include radio communication and navigation, satellite communication, and broadcasting.

12 "Health" may include healthcare, medical and hospital care, and medicines and vaccines.

13 "Transportation" may include land, air, maritime, rail, inland waterways, ocean and short-sea shipping and ports, and logistics.

[14] “Food” may include agriculture and grocery.

[15] “Security” may include national defense.

[16] “Chemical sector” may include production and storage/processing of chemical substances and pipelines of dangerous goods (chemical substances).

[17] “Dams” may include water retention and control services as defined by the United States; separate from the water sector.

[18] Metropolitan centers can be defined, classified, and updated by the National Economic Development Authority or the Philippine Statistics Authority.

[19] “Personal information,” as defined in the Philippine Data Privacy Act of 2012 and used in this publication, refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

[20] “Processing” refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data. See Section 3(j), Data Privacy Act (2012). “Personal information” refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. See Section 3(g), Data Privacy Act (2012).

[21] For more information, see Memorandum Circular No. 18, s. 2020 (Civil Service Commission, 2020).

[22] See Office of the Court Administrator Circular 100-2020, Administrative Circular No. 40-2020, Office of the Court Administrator Circular 89-2020, Administrative Circular No. 39-2020, Administrative Circular No. 33-2020, and Administrative Circular No. 37-2020 (Supreme Court of the Philippines, 2020b, 2020c, 2020d, 2020e, 2020f, and 2020g).

[23] “Electronic government,” also known as e-government, is the provision of public services via the Internet, or more generally, the use of digital technology in support of government activities and processes. Also referred to as e-governance.

[24] As of 2016, all functions of the Department of Transportation and Communication relating to communications have been transferred to the DICT. The National Computer Center was abolished, with their powers and functions transferred to the DICT. The NTC, on the other hand, is now an attached agency of the DICT for policy and budget purposes.

[25] In the amendments to the Revised Rules on Evidence issued by the Supreme Court (2020a), “the introduction and appreciation of electronic evidence were further refined” (p. 2). Also, see examples: *NAPOCOR v. Codilla* (2007), *MCC Industrial Sales v. Ssangyong Corp.* (2007), *Torres v. PAGCOR* (2011), and *People v. Enojas* (2014).

[26] To apply for digital certificates, go to https://dict.gov.ph/pnpki-agency-certificate/ for government and nongovernment entities and to https://dict.gov.ph/pnpki-individual-certificate/ for individual citizens. To apply for Secure Sockets Layer (SSL) certificates for computers, servers, and machines, go to https://dict.gov.ph/pnpki-ssl-certificate/.

[27] See Section 7 of Ease of Doing Business and Efficient Government Service Delivery Act (2018).

[28] PHP is an open-source, general-purpose scripting language that is especially suited for web development and can be embedded into HTML (PHP.Net, n.d.).

[29] In the first quarter of 2019, more than half of phishing sites were using SSL certificates (Interpol, 2021).

30 According to We Are Social and HootSuite, there are 4.2 million new Internet users in the country, an increase of 6.1% from January 2020 to January 2021 (Kemp, 2021).

31 Using digital payments regularly is defined as "active accounts making at least one transaction per month" (Massally, et al., 2019). In 2019, the BSP set a target of driving the share of digital payments to 20% by 2020 (Villanueva, 2020). But with the mobility restrictions under quarantine conditions during the pandemic, actual figures might exceed this target.

32 InstaPay is designed for urgent and small value transactions (BSP, 2020b). On the other hand, PESONet is designed for high-value transactions of companies, other businesses, government agencies, and individuals. It is the electronic alternative for transferring funds via checks (BSP, 2020c).

33 According to a report by *TechWire Asia*, GCash "had to upsize its e-wallet limits" in April 2020 in order to accommodate a growing user base doing online transactions (Devanesan, 2020). Its competitor, PayMaya, also partnered with local governments, like the City of Manila, for contactless payment.

34 According to BSP Governor Benjamin Diokno, this is part of the BSP's "FinTech roadmap that is crafted to nurture a regulatory environment that allows innovations to flourish, yet still mindful that risks must be effectively managed and that the financial system remains safe and sound" (Diokno, 2019).

35 The BSP, through the Financial Inclusion Steering Committee, supports House Bill No. 8910 or the proposed Open Access in Data Transmission Act, which aims to promote the expansion of the country's digital infrastructure.

36 "Telemedicine" is the use of ICT to provide medical services remotely. Telemedicine is most closely associated with remote doctor's consultation (World Health Organization, 2010).

37 "Interoperability" refers to the ability of contact-tracing apps to exchange minimum information necessary, so users are alerted if they have been in proximity with another user who has tested positive for COVID. This should be applicable wherever the user is in the EU. See European Commission (2020, p. 3).

38 See, for example, NPC's guide on the proper handling and protection of personal data collected from customers and visitors, which include (1) collecting only what is necessary; (2) being transparent; (3) using information only for the declared purposes; (4) implementing security measures; and (5) keeping the data only for a limited time (NPC, 2020).

39 See, for example, DICT Department Circular No. 003 s. 2020, which established the Philippine National CERT or CERT-PH (DICT, 2020).

40 The Philippines' water laws include: PD 1067 Water Code (1976); PD 198 Provincial Water Utilities Act (1973); PD 522 Prescribing Sanitation Requirements for the Travelling Public; RA 7586 National Integrated Protected Area System Act (1992); RA 8041 National Water Crisis Act (1995); RA 8371 Indigenous Peoples Rights Act (1997); RA 9275 Clean Water Act (2004); and RA 8435 Agriculture and Fisheries Modernization Act.

41 Agencies with a role in water resources include the following: NEDA (policymaking and planning); National Water Resources Board (coordination and regulation), Department of Environment and Natural Resources (DENR), DOH, Department of Interior and Local Government (DILG), Department of Public Works and Highways (DPWH) (water quality and sanitation); Department of Agriculture (DA), NPC, DENR (watershed management); Board of Investments, Philippine Economic Zone Authority (PEZA) (integrated area development); National Anti-Poverty Commission–Water Supply Coordination Office, Department of Finance–Cooperative Development Authority, DPWH, Housing and Urban Development Coordinating Council, DILG, PEZA (water supply); National Irrigation Authority (irrigation); DOE, Power Sector Assets and Liabilities Management Corporation, NPC, Philippine Electricity Market Corporation (hydropower); DPWH, Office of Civil Defense, Department of Science and Technology (DOST), Metro Manila Development Authority (flood management); Philippine Ports Authority (ports); Bureau of Fisheries and Aquatic Resources, Philippine Tilapia Association (fisheries); NWRB, DOH, DPWH, DENR, DOST (data collection); DOST, DENR (research); DA (cloud seeding) (Alikpala & Ilagan, 2018, p.9).

42 These are government-owned airports that are classified by the Civil Aviation Authority of the Philippines as international airports, principal or domestic airports (Class 1 or Class 2), or community airports. See Bureau of Fisheries and Aquatic Resources (2013).

43 "Application programming interface," or API, is a software intermediary that allows two applications to talk to each other (Red Hat, 2017). In e-government, API refers to a set of commands, functions, and protocols that allows organizations, such as the government, to create software that will expose capabilities of a particular e-government service to other services or application developers, thus allowing third parties to embed e-government capabilities into their own applications and enable multiple services and applications to provide a particular e-government service.

44 Also, see Memorandum Circular No. 005 s. 2017 on the protection of critical information infrastructure (DICT, 2017b).

45 PhilID is the third component of the PhilSys, the other two being the PhilSys Number and the PhilSys Registry. See Sections 6 and 7 of the Implementing Rules and Regulations of the Philippine Identification System Act (PSA, 2018).

46 The Social Amelioration Program had a budget of PHP 205 billion to be distributed to 18 million families at the rate of PHP 5,000 to PHP 8,000 per family, depending on the region.

47 The core technological infrastructure of the PhilSyS is made up of four components: (1) registration kits, (2) automated biometric identification system, (3) systems integrator, and (4) card production (PSA, 2020b).

48 As of July 15, 2021, only 4.2 million individuals had registered (PSA, 2021a).

49 Data is being collected separately by the Bureau of Internal Revenue, SSS, GSIS, Philippine Health Insurance Corporation (PhilHealth), and Commission on Election (COMELEC), among others.

50 Section 11 of the Data Privacy Act provides, "The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality."

51 Section 5(e) of RA 8792 or the e-Commerce Act defines electronic signature as "any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document."

52 The right to information includes access to "official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development." See Section 7, Article 3 of the Philippine Constitution (Const., 1987).

53 "Cloud services provider" is an entity in the business of providing cloud services, such as a platform, infrastructure, application, or storage services, to other organizations. Refer to *Cloud Services* in Chapter 1 for a more detailed explanation.

54 Lack of training makes an organization vulnerable to attacks. The training, however, "must be tailored to the needs and responsibilities of individuals, teams, and departments," which would be more effective than generic security advice (Whitney, 2020).

5 Findings and Recommendations for Improving Cybersecurity in the Philippines

> *Cybersecurity needs to be a key priority of the Philippines if it intends to participate more meaningfully in, and benefit from, the fast-growing global digital economy.*

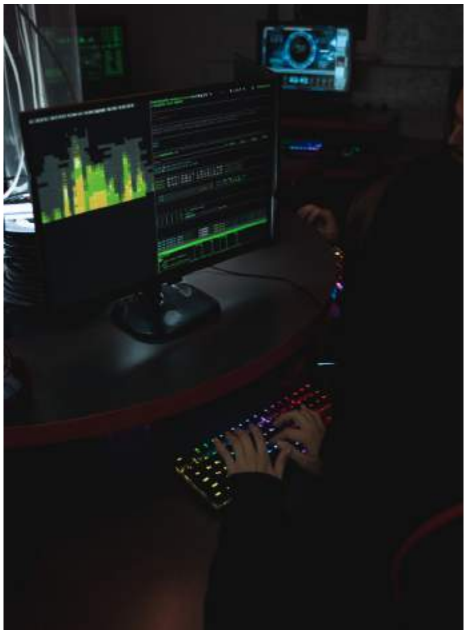
The Internet is a transformative tool that allows the sharing of information at a pace and scope faster and larger than the world has ever seen before. It has enabled the distribution of economic opportunities globally, helping countries leapfrog development and achieve growth rates faster than those of the economies that thrived during the past industrial revolutions.

The COVID-19 pandemic, which forced the world to impose lockdowns, accelerated the digitalization process for many developing nations, including the Philippines. Businesses continued operation on a work-from-home arrangement. E-commerce was at an all-time high. Most of the companies who were able to adjust and survive the mobility restrictions were those who embraced e-commerce. With more Internet transactions, online banking and digital payments also increased exponentially. Face-to-face classes were suspended, and about 28 million Filipino students (and their families) were forced to stay home and shift to remote learning. Related industries that supported the shift to digital solutions, like logistics, warehousing, telecommunications, Internet, and information technology and cloud services, also grew.

With the rapid growth of the digital ecosystem also came a significant increase in information security risks and an expansion of the threat landscape. More digital use and users means more personally identifiable information, financial transactions, online databases, and other vectors for exploiting individuals and organizations that are available for cybercriminals. Malware or malicious software, phishing and spoofing, ransomware, e-commerce data interception, cyber scams, information leakages, cryptojacking and crimeware-as-a-service are just some of the cybercriminal activities that have intensified since 2020. Today, cyber threats and risks are a regular part of people's daily lives—just the like COVID-19—whether they are aware of it or not.

Cybersecurity issues started out as individual pranksters and petty criminals exploiting the vulnerabilities of information and communications technology (ICT) systems and cyberspace. Through the years, cyberattacks have evolved to become a very lucrative venture for malicious cyber actors and a very costly problem for organizations. In 2020, Cybersecurity Ventures, a cyber economic market data analytics company, estimated that cybercrime would inflict damages amounting to USD 6 trillion globally in 2021 and that cost would rise to as much as USD 10.5 trillion by 2025 (Morgan, 2020).

That some of the most prominent cyber incidents involved sophisticated, highly organized, and well-funded state actors today has made cybersecurity a political issue. Warfare is now fought in cyberspace, and the nation with the best digital arsenal can now be considered a global superpower. Geopolitics has indeed infiltrated cyberspace, engendering conflict over which set of values should be embedded in the world's technologies, networks, and systems. It now defines the two main approaches to cybersecurity: the West-led bottom-up approach promoted by the United States and the European Union, and the top-down approach championed by China and its allies. For the countries caught in between, buying into a particular technology or system is deemed equivalent to aligning with one side of the debate—and disengaging with the other.



The definition of "secure" increasingly lies on which side one belongs and which technology one is using. This has practical consequences on who can access networks tied to global banking, finance, and trade, among others, as seen in the American Clean Network Initiative. Clearly, the technological superpower that a country sides with and the security approach it adopts will be an economic security policy issue that will affect the nation's general welfare.

There are, however, other state actors and various types of government actions and decisions that affect how people access and experience the Internet. Far from being bystanders to the innovation and business models the big tech giants churn out, governments are now trying to take control over another jurisdiction—cyberspace. Thus, the Internet now is very different from the Internet from years ago, with one country having its own sets of rules and regulations on what citizens can and cannot access, often in the name of security and data privacy. In a fragmenting Internet, states increasingly impose rules and regulation on content and technologies that their citizens can access and use based on their own national interest. Thus, the free flow of information and global cooperation, principles upon which the Internet was built, are now under threat. And how countries view the Internet affect their general approach to cybersecurity.

In the Philippines, cybersecurity is not seen as a priority yet. **Because the country is still at the initial stage of digital transformation, there seems to be a misconception that threat actors do not pose as serious a threat or that the Philippines is not a target**. This mindset can affect decisions about investing in cybersecurity, especially in the public sector, which makes the country all the more vulnerable to various forms of cyber threats and attacks. It needs to be emphasized that cybersecurity threats can be "indiscriminate and broad-based, designed to exploit the interconnectedness of the Internet." The general lack of investment in cybersecurity can, thus, lead to economic losses at the individual and aggregate levels (Internet Policy Task Force, 2011).

Cybersecurity needs to be a key priority of the Philippines if it intends to participate more meaningfully in, and benefit from, the fast-growing global digital economy. The quality of this participation is directly related to the level of trust that a trading partner has with the Philippines. The country has always endeavored to move its local enterprises up the global value chain. In an interconnected world, the Philippines will be confined to processing low-value commodities if it does not enhance its information security game because highly developed economies will not entrust it with sensitive data for processing. Data as the "new oil" should be treated as a resource that impacts economic development. This resource is destroyed or devalued each time a successful hack occurs, or a leakage happens, especially when inflicted on critical infrastructure or databases of key government agencies. Thus, the country must ensure that data is secured and protected at all times. This entails investing in people, technology, and processes.

The Philippines needs to create a responsive institutional arrangement for cybersecurity. Effective cybersecurity governance means that each government agency manages and protects its information security and recognizes that, like digitalization, cybersecurity should be part and parcel of its responsibility. It is important that cybersecurity initiatives be considered a priority of the top management of government agencies, especially those that operate critical infrastructure. Support for cybersecurity can be in the form of adherence to internationally accepted cybersecurity standards and issuance of organizational policy and protocol to protect information security. Cybersecurity programs must also be given the necessary budget to purchase technology solutions and, more importantly, to continuously train people and build the capacity of the institution to identify, respond, and prevent cyber incidents.

It is recommended that the Department of Information and Communications Technology, together with the National Cybersecurity Interagency Committee, lead in developing the cybersecurity posture of the country through the crafting of a national cybersecurity framework and strategy. The ICT department will assess the appropriateness and prescribe relevant information security standards, provide technical support and expertise, help build the capacity of various agencies, and promote a whole-of-government approach to protecting and promoting information security. The same standards must apply to members of the private sector that work with the government.

Recommendations

Given the different issues that impact cybersecurity, this report recommends the following solutions that will address the cybersecurity knowledge, policy, and skills gaps in order to improve the Philippines' cybersecurity posture:

Knowledge gap

1. Create greater awareness of the global and local cybersecurity context and a better appreciation of the threat landscape.
2. Generate and analyze local data on cybersecurity practices and incidents on a sectoral level in order to identify security gaps, inform decisions and policy, and provide appropriate solutions.
3. Nurture an environment of cooperation and information sharing among the local and international cybersecurity communities because one's incident can be another's lesson.

Policy gap

4. Adopt policy enforcing minimum information security standards to protect critical information infrastructure and the ICT systems of public institutions.

Skills gap

5. Develop a cybersecurity culture by raising awareness, supporting training and capacity building for cybersecurity talent, and instilling cybersecurity as a way of life through educational institutions.

> **The country must be equipped with information and an understanding of what is happening outside as much as within the country's cyber threat landscape.**

Below is a more detailed description of the key recommendations:

1. **Create greater awareness of the global and local cybersecurity context, and a better appreciation of the threat landscape, in order to improve the Philippines' cybersecurity posture.**

   The first step to effectively responding to various cybersecurity challenges is to address the ***cybersecurity knowledge gap***. The country must be equipped with information and an understanding of what is happening outside as much as within the country's cyber threat landscape. Examining the cybersecurity policy and practices of other countries can provide insights into how the Philippines should position itself.

   In the case of the U.S. Clean Network Initiative, for example, the Philippines must take proactive steps to provide global firms with the necessary assurances and protections that its ICT infrastructure and cybersecurity policies provide adequate security for investors. With 75% of the USD 23 billion business process outsourcing services catering to the United States (Morales & Lema, 2016), the Philippine government has to actively play a part in enforcing these assurances that data and the transmission of such are safe in the Philippines. Being a member of the International Telecommunication Union, the Philippines may also express an active voice in protecting fundamental democratic rights, such as privacy and expression, as technologies evolve.

Local businesses, private organizations, and even individuals must also be cognizant of the emerging divisive digital lines. With certain countries disallowing strong encryption, the simple act by a local private enterprise of choosing a network protocol might have ramifications to its business and available markets. Individuals should be careful when selecting apps, services, and devices and be conscious about the countries that manufacture them—whether they align with their home country's laws and regulations, operating under norms that are inconsistent with the democratic values under which the Philippines operates. For example, the providers of popular chat services may be operating under different standards from what is considered as legal state interception or levels of encryption—a matter that Filipino users should be conscious about.

2. **Generate and analyze local data on cybersecurity practices and incidents on a sectoral level in order to identify security gaps, inform decisions and policy, and provide appropriate solutions.**

The Philippines has made some strides in addressing cybersecurity challenges by passing laws on data privacy protection and cybercrime prevention. However, compared to other ASEAN countries, the country still ranks poorly in terms of cybersecurity. To improve its cybersecurity posture, the Philippines needs to assess its current situation and identify the various risks and threats that may affect the nation. This can only be done by collecting local cybersecurity data from various organizations and stakeholders.

Anne Neuberger, deputy national security advisor for Cyber and Emerging Technology at the White House, once said that a significant cyber incident is "an opportunity to focus on the core issues that led to these cyber incidents" and "help everyone improve their security" (Palmer, 2021).

In the case of the Philippines, data on cyber incidents from sectoral computer emergency response teams (CERTs) can be very valuable and helpful in identifying the various threats, formulating solutions to address these threats, as well as putting preventive measures in place. A survey on cybersecurity in public institutions, such as the one the Department of Information and Communications Technology initiated in 2021 with *Secure Connections*, would also help assess the state of cybersecurity within the government and provide insights into current practices and policy, issues and gaps, and improvements over time, if any.

3. **Nurture an environment of cooperation and information sharing among the local and international cybersecurity communities because one's incident can be another's lesson.**

Effective cybersecurity governance extends beyond public institutions to address the risks posed to other sectors, especially those with critical infrastructure. The intertwining of digital systems in areas such as banking, healthcare, and telecommunications, for example, presents a risk to effectively governing the country should a cybersecurity catastrophe lead to the failure of these sectors. Also, cybersecurity threats do not recognize borders or boundaries. Threat actors can take advantage of any vulnerable target anywhere in the world. Thus, it is important to have an environment where local and international communities cooperate and exchange relevant information that can help prevent cyber incidents or provide possible solutions to a similar incident being experienced by other groups. Information sharing also helps in building the body of knowledge and understanding of the global and local context, which in itself is an important solution to the cybersecurity knowledge gap.

> **Compliance to minimum information security standards is a prerequisite to digital transformation.**

4. **Adopt policy on minimum information security standards to protect critical information infrastructure and the ICT systems of public institutions.**

Establishing a baseline of what information security mechanisms the country has and what it should have, at the very least, is important in assessing the gap and how certain potential cyberattacks would affect the Philippines. Equally important is identifying the country's level of information security risks and vulnerabilities and how it should respond given certain types and levels of threats.

The first crucial step is to address the cybersecurity policy gap. Currently, there are department orders on information security, but implementation has been a challenge. A policy enforcing a minimum level of information security protection for critical infrastucture and all public institutions can be in the form of an executive order that

- requires compliance with minimum information security standards for all government agencies, with a more stringent set of requirements imposed on institutions, whether public or private, that own and/or operate critical infrastructure;
- mandates government agencies to put information security mechanisms in place in order to prevent and respond to cyber threats and incidents in their respective sectors or jurisdictions;

- directs all agencies, through the sectoral CERTs, to submit data on cyber incidents to a centralized reporting mechanism that is maintained by a national CERT; and
- mandates each government agency to designate a cybersecurity trained and accredited personnel as part of top management, who can help the organization make decisions about cybersecurity, monitor the organization's compliance with information security standards, and encourage institutional capacity building.

As countries like the Philippines aim to digitalize various key sectors, a parallel, simultaneous effort needs to be made to ensure the protection of ICT systems and networks, especially those that carry personal data, sensitive information, and are connected to the public Internet. These standards, however, must be translated to actual processes and accepted as part of the norm.

Compliance with minimum standards can help prevent information security incidents or lessen their impact. When cybersecurity indicidents occur—and it is guaranteed that they will—having minimum information security requirements helps set a baseline for a proper response and promotes transparency and accountability, particularly in government. When an incident, such as data leakage, happens, compliance with basic protocol can help determine whether a government agency applied due care, the possible shortcomings and gaps that need to be addressed, and what its liabilities are, if any.

However, minimum standards are only a start. Further policies and recommendations can be enhanced to support more stringent cybersecurity controls on a sector or risk basis. Information security governance is a cycle that aims to be enhanced per iteration, so this is a continuous process.

The country needs to foster a credible enforcement environment where the chain of command and accountabilities in each organization, especially in government, are clearly defined; data sharing and reporting of information security incidents are done in an appropriate, timely, and consistent manner; and noncompliance, particularly those that are proven to result in successful cyberattacks and increased level of risk, is met with consequence. There is often more incentive for organizations to act when the consequence has a direct impact on them. For example, private sector contractors who perform an outsourced function on behalf of the government must be aware of, and comply with, all the basic information security requirements. The principal government agency is still primarily responsible for ensuring that the appropriate information security mechanisms are in place and shall be accountable for when an information security incident occurs. However, the private company also faces the possibility of having its regulatory licenses and permits revoked for negligence or noncompliance to standards.

> **Ultimately, the goal is to make cybersecurity everyone's responsibility.**

5. **Develop a cybersecurity culture by raising awareness, supporting training and capacity building for cybersecurity talent, and instilling cybersecurity as a way of life through educational institutions.**

   Based on the various cyber threats that are on the rise and continue to evolve, building the capacity and expertise of a country's human resources will make a huge difference. In security incidents, people are often the weakest link. No amount of advanced technology can replace or make up for cybersecurity-capable personnel. Thus, it is crucial that capacity building of people is continuous and that developing a cybersecure mindset is part of the overall culture. This way, protecting against cyber threats becomes instinctive to institutions and their people.

   Developing a cybersecurity culture will require institutionalizing information security and promoting the discipline not only through training but also as part of formal education. In many countries, for example, courses in cybersecurity are already a regular offering in schools and universities. The Philippines can partner with these countries to help develop the curriculum for information security and nurture information security professionals. Including cybersecurity as a course in higher education is one way of creating a pool of locally trained cybersecurity experts and, eventually, address the ***cybersecurity skills gap***.

   Ultimately, the goal is to make cybersecurity everyone's responsibility. Each government agency must develop its own cybersecurity strategy and capacity. Each sector is encouraged to have its own standards that are relevant to its needs and requirements. Each institution, whether public or private, ought to adopt an organizational policy and protocol for their daily operations and employees' individual tasks. Each household must make cybersecurity a habit.

   Armed with an understanding of the realities of cybersecurity, the challenge now is in identifying and implementing what adaptations the Philippines can make at the state, organization, and individual levels to mitigate cybersecurity risks and to become cyber resilient. How the Philippines answers this question has profound implications on its evolving relations with its global peers, how its institutions will effectively and securely use technologies, how its businesses and workforce will participate in the digital economy, and how its citizens will live and thrive safely and securely in a digital world.

GLOSSARY

A

Antivirus software

Also known as *anti-malware*, software especially designed to monitor devices, systems, and networks for the presence of malware, addressing them automatically and alerting administrators as appropriate. See also *Malware*.

Artificial Intelligence (AI)

Intelligent machines or computer programs that process information with minimal human input and are therefore capable of independent analysis, forecasting, and problem-solving. Also used to describe the field of study and technological development involving the creation of machines that can learn from experience and adjust to new inputs with human-like acuity. See also *Machine Learning*.

Application Programming Interface (API)

A software intermediary that allows two applications to talk to each other. In e-government, API refers to a set of commands, functions, and protocols that allows organizations, such as the government, to create software that will expose capabilities of a particular e-government service to other services or application developers, thus allowing third parties to embed e-government capabilities into their own applications and enable multiple services and applications to provide a particular e-government service.

Attack vector

A method or pathway used by a hacker to access or penetrate a computer or network, by exploiting some vulnerability in the system. Attackers may use one or multiple vectors to steal data, infect systems with malware, or some other criminal aim.

Authentication

The process of verifying the identity of a user, process, or device before providing access to a secured network or system.

B

Bandwidth, or Internet bandwidth

Maximum “speed” or amount of data that can be transmitted over an Internet connection.

Breach

Any situation where an actor gains unauthorized access to a system, network, or device, often resulting in the loss or compromise of information. Also called *data breach* or *security breach*.

Bring Your Own Device (BYOD)

The practice of allowing organization members to use personal devices to access the organization’s network and other IT resources. This is contrasted with the traditional approach of issuing dedicated work devices to employees that serve as their only points of access to the network.

Business Email Compromise (BEC)

A type of cybersecurity attack that involves manipulating employees into transferring money or information to criminals, using the hijacked or spoofed business email addresses of an organization’s leadership. The objective of the malicious actor is often to defraud a company.

C

Cloud security

The set of policies, controls, procedures, and technologies that protect cloud-based systems, data, and infrastructure. One of the key areas of cloud security is authorization or ensuring that only intended users have access to the cloud network or asset.

Cloud services

The use of servers accessed through the Internet, as opposed to an organization’s own on-premises servers, to host the organization’s applications, data, and services. As the Internet allows for multiple points of connection, it is possible for a cloud server to provide services to more than one organization, or for an organization to obtain cloud services from a third-party provider. Cloud services can thereby help minimize business overhead related to maintaining a network, making them a popular option for organizations.

Cloud services provider An entity in the business of providing cloud services, such as a platform, infrastructure, application, or storage services, to other organizations. See *Cloud Services*.

Credential dumping The extraction of usernames and passwords from a device's memory using specially created malware.

Crimeware-as-a-Service (CaaS) The criminal business model of selling cyberattack expertise to other criminals.

Critical infrastructure Assets, systems, and networks, whether physical or virtual, that are considered so vital that their destruction or disruption would have a debilitating impact on national security, health and safety, or economic well-being of citizens, or any combination thereof. Examples include the banking system, oil pipelines, water systems, and electricity systems.

Critical services Any service critical to widespread order, security, and functioning. See also *Critical Infrastructure*.

Cryptography Techniques intended to secure data and systems from unauthorized access, using codes, passwords, and authentication mechanisms, as well as provide security guarantees like confidentially, integrity, availability and nonrepudiation.

Cryptojacking A type of malware attack that takes over or hijacks computer systems and uses them to "mine" for cryptocurrencies.

Cyberattack Any malicious activity aimed at stealing, manipulating, disabling, or otherwise disrupting a network, system, or information in a targeted manner.

Cybersecurity The state of having secure data, systems, networks, and other ICT assets, protecting them from malicious attacks and any other threats to their integrity.

Cybersecurity framework

The system of concepts, rules, and practices dictating the direction of policies and regulations, including the implementation of legal, technical, and political tools to align with the overall goals of a country or other entity.

Cybersecurity governance

The approach by which a country, organization, or some other entity monitors, evaluates, and ensures the protection of information, ICT systems and networks, and digital assets. See also *Cybersecurity Framework*.

Cybersecurity measures

Implementation of techniques, methods, or policies designed to improve an entity's cybersecurity posture.

D

Dark web

A general term used to describe Internet sites that are hidden behind specialized security protocols, designed to anonymize users and web hosts alike. These websites often act like private networks, requiring specific software or network configurations to gain access. For this reason, the dark web is often used for illicit activities by cybercriminals.

Data leakage

Any instance of access to data by unauthorized entities from within or outside an organization, whether accidental or intentional. See also *Breach*.

Data privacy

The concept of securing personal information or any other sensitive data from unauthorized access and use. As a *legal right*, data privacy is a person's right to control any data about or originating from them.

Digitization

The process of converting analog information to digital formats, such as from paper records to computer-based ones.

Digitalization

The shift of content, processes, operations, and activities to computer- and/or Internet-enabled forms. Also used to describe the work of transforming objects and assets from the physical world into digital form to take advantage of ICT's transformative potential for business or activity models.

Domain Name System (DNS)

A part of the Internet infrastructure responsible for identifying computers, services, or other resources connected to the Internet, each of whom are assigned *domain names*.

Domain Name System (DNS) poisoning

A type of cyberattack that involves compromised domain names, allowing attackers to trick users into visiting arbitrary hosts defined by them in lieu of their intended destinations, effectively redirecting traffic. See *Domain Name System*.

E

Education Technology (EdTech)

A broad range of technologies, such as software or Internet platforms, designed for use in an education setting. EdTech can also refer to teaching and learning practices that use ICT.

Electronic commerce (e-commerce)

The general concept of conducting commercial activities via the Internet.

Electronic government (e-government)

The provision of public services via the Internet, or more generally, the use of digital technology in support of government activities and processes. Also referred to as *e-governance*.

I

Information and Communications Technology (ICT)

A family of related electronic, primarily digital technologies, that enable access to vast amounts of stored information, or the transfer of data between users. A common thread among ICTs is that they allow users to interact with data—send, receive, process, and store it, to name a few activities.

Information leakage

As used in this publication, a type of data leakage that involves a software's unintended release of sensitive data to unauthorized persons due to faults in the software. See also *Breach, Data Leakage*.

Information security

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Internet Protocol (IP)

The set of rules for routing and addressing packets of data so they can travel across the multiple networks making up the public Internet. IP ensures that data packets arrive at the right destination. To identify devices connected to the Internet for routing purposes, all these devices are given an identifier called an *IP address*.

Internet-of-Things (IoT)

The Internet-enabled network of smart devices facilitating machine-to-machine (M2M) communication, without the need of human interference. See *Smart Devices*.

M

Machine learning

A software paradigm involving the use of large data sets to "train" or improve the software's processing and interpretation of data.

Malicious actor

A catch-all term for any entity, from nation-state backed groups to rogue individuals, that aims to infiltrate or attack another entity's ICT assets for their own ends. Also called *bad actor* or *threat actor.*

Malware

Shorthand for malicious software, or any software designed to harm or exploit a device or network.

N

National ID

Refers primarily to PhilSys, the Philippine identification card and system mandated by law under Republic Act No. 11055, otherwise known as the Philippine Identification System Act, and operated by the Philippine Statistics Authority. May also refer to similar schemes or systems from other countries.

National security

Refers to the protection and defense of a country's citizens and their well-being, both physically and economically. Issues affecting national security can be national in *scope* if they directly affect a large number of persons in the country, or in *impact* if the consequences thereof have implications for a significant proportion of the country.

P

Personal information

As defined in the Philippine Data Privacy Act of 2012 and used in this publication, any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Phishing

A specific kind of spoofing cyberattack that lures victims into providing personal or sensitive information, such as birthdates and addresses, credit card details, or passwords. The attackers then use this information for other malicious purposes, such as gaining access to bank accounts or infiltrating a network or system. See *Spoofing*.

R

Ransomware

A subtype of malware that hijacks systems and prevents access to part or all of an organization's data, unless a ransom is paid to the criminal group behind the ransomware.

Remote learning

The practice of conducting classes and other traditionally school-bound activities from a distance, using a mix of ICT and traditional technologies such as printed modules. Also known as *distance learning*.

Request for Comment (RFC)

A stakeholder-driven development process, commonly associated with the Internet Engineering Task Force's standards development, that allows anybody to propose technical specifications or standards to be used on the Internet. All RFCs are published online and are adopted on a voluntary basis.

S

Sensitive data

As used in this publication, any data access which can compromise the security of a person, organization, or any entity. In data privacy, "sensitive personal data" is any information revealing an individual's racial or ethnic origin, marital status, age, and religious, philosophical or political affiliations; their health, education, genetic [information] or sexual life; information issued specifically to an individual by the government, such as social security number; or any other information fundamental and traceable to that individual's identity.

Smart device

A general term for any Internet-connected device capable of receiving, processing, and transmitting data on its own, using what is known as *machine-to-machine* (M2M) communications. See also *Internet of Things*.

Spoofing

Any type of cyberattack that involves tricking the victim into believing an email, website, or other communications is from a trusted contact or organization, such as a bank or school. Examples include websites designed to look like online banking pages, or fraudulent emails that purport to be from a school or government body.

T

Telemedicine

The use of ICT to provide medical services remotely. Telemedicine is most closely associated with remote doctor's consultation.

V

Virtual Private Network (VPN)

The use of security protocols and technologies to allow access to an organization's private servers through the public Internet, as if the user was on-site and directly connected to the network. More generally, VPN can also refer to any private network running over the Internet. In the latter case, VPNs can be used to disguise or obfuscate the contents and origins of Internet traffic, whether from organizations or individual users.

Virtual Private Network (VPN) Provider

Any entity who hosts or operates a VPN for other entities, such as organizations or individuals. See *Virtual Private Network*.

Virtualization

Involves the compartmentalization of systems or network resources on a single physical device, ensuring users are unable to access other users' information.

Virus

Malware that "infects" software or systems if a user runs the malware on their device, allowing the virus to spread itself to other parts of a system or network. See also *Worm*.

Vulnerability

In cybersecurity, any flaw or oversight in a device's, system's, or network's design, whether physical, technological, or even social, that can be exploited by attackers to do harm.

W

Work-From-Home (WFH)

A broad range of systems and methods for bringing traditionally office-bound work activities elsewhere, whether fully or partly. Also called *remote work, telework, or home-based work*.

Worm A type of malware that has the ability to infect software or systems without user input, and self-propagate itself secretly across a network. See also *Virus*.

Z

Zero trust A network security approach that considers all users and devices “untrusted” by default, only providing access as-needed to properly verified users.

IMAGES / PHOTOS CREDITS

Introduction cover photo:
From Barbhuiya, T. (2021). Unsplash (https://unsplash.com/photos/FnA5pAzqhMM). In the public domain.

Part 1 cover photo:
From NASA. (2015). Unsplash (https://unsplash.com/photos/Q1p7bh3SHj8). In the public domain.

Chapter 1 cover photo:
From Goldstein, A. (2019). Unsplash (https://unsplash.com/photos/EUsVwEOsblE). In the public domain.

Chapter 2 cover photo:
From Dhage, S. (2021). Unsplash (https://unsplash.com/photos/UxDU0Gg5pqQ). In the public domain.

Chapter 3 cover photo:
From Carra, G. (2020). Unsplash (https://unsplash.com/photos/gf6UDwpl0ac). In the public domain.

Part 2 cover photo:
From FLY:D. (2021). Unsplash (https://unsplash.com/photos/mT7lXZPjk7U). In the public domain.

Chapter 4 cover photo:
From Buillerey, M. Unsplash (https://unsplash.com/photos/tKiaYOzmszQ). In the public domain.

Chapter 5 cover photo:
From van Dijk, E. Unsplash (https://unsplash.com/photos/uAWRPtZ6n0s). In the public domain.

page 17:
From Antonaidou, N. (2020). Unsplash (https://unsplash.com/photos/9X1P46Y2KJo). In the public domain.

page 18:
From athree23. (2018). Pixabay (https://pixabay.com/images/id-3692440/). In the public domain.

page 19:
From Park, T. (2020). Unsplash (https://unsplash.com/photos/6MePtA9EVDA). In the public domain.

page 20:
From vickygharat. (2020). Pixabay (https://pixabay.com/images/id-5332676/). In the public domain.

page 22:
From Baumeister, M. (2021). Unsplash (https://unsplash.com/photos/WqZwkrBuZIE). In the public domain.

page 27:
From NASA-Imagery. (2010). Pixabay (https://pixabay.com/images/id-986/). In the public domain.

page 30:
From TheDigitalArtist. (2018). Pixabay (https://pixabay.com/images/id-3866609/). In the public domain.

page 32:
From Yang, L. (2016). Unsplash (https://unsplash.com/photos/5h_dMuX_7RE). In the public domain.

page 34:
From TheDigitalArtist. (2017). Pixabay (https://pixabay.com/images/id-2254769/). In the public domain.

page 36:
From geralt. (2017). Pixabay (https://pixabay.com/images/id-2910624/). In the public domain.

page 37:
From Sar, T. (2018). Unsplash (https://unsplash.com/photos/T01GZhBSyMQ). In the public domain.

page 41:
Note: From Woroniecki, J. (2020). Pixabay (https://pixabay.com/images/id-5319462/). In the public domain.

page 43:
From del Olmo, I. (2018). Unsplash (https://unsplash.com/photos/NIJuEQw0RKg). In the public domain.

page 45:
From Goodman, J. (2019). Unsplash (https://unsplash.com/photos/Oalh2MojUuk). In the public domain.

page 52:
From Social Estate. (2017). Unsplash (https://unsplash.com/photos/P-t9yap_20M). In the public domain.

page 54:
From Joshi, A. (2019). Unsplash (https://unsplash.com/photos/KiZSGUZ5NMk). In the public domain.

page 56:
From Tang, L. (2019). Unsplash (https://unsplash.com/photos/yBroAF1cN3I). In the public domain.

page 57:
From Luengo, A. (2019). Unsplash (https://unsplash.com/photos/jL0tMFYOdBM). In the public domain.

page 59:
From Clancy, L. (2021). Unsplash (https://unsplash.com/photos/B5MBc6fK0WY). In the public domain.

page 61:
From Pixabay. (2016). Pexels (https://www.pexels.com/photo/security-logo-60504/). In the public domain.

page 62:
From Nayda, O. (2019). Unsplash (https://unsplash.com/photos/IBQw38N-6fM). In the public domain.

page 66:
From thekurupi. (2016). Pixabay (https://pixabay.com/images/id-1788706/). In the public domain.

page 69:
From Feliciotti, A. (2021). Unsplash (https://unsplash.com/photos/MCWONeEXhC4). In the public domain.

page 70:
From Arya, N. (2018). Unsplash (https://unsplash.com/photos/5i3oyOrojvk). In the public domain.

page 74:
From Tumisu. (2016). Pixabay (https://pixabay.com/images/id-2321665/). In the public domain.

page 80:
From Sikkema, K. (2019). Unsplash (https://unsplash.com/photos/M98NRBuzbpc). In the public domain.

page 82:
From iGov Philippines. (n.d.). *Integrated Government Philippines Program*. https://i.gov.ph/.

page 83:
From mohamed_hassan. (2021). *Pixabay* (https://pixabay.com/images/id-6693816/). In the public domain.

page 86:
From Shvets, A. (2020). Pexels (https://www.pexels.com/photo/person-holding-bank-card-4482900/). In the public domain.

page 87:
From B_A. (2018). Pixabay (https://pixabay.com/images/id-3342696/). In the public domain.

page 92:
From mohamed_hassan. (2021). Pixabay (https://pixabay.com/images/id-6573326/). In the public domain.

page 94:
From Winkler, M. (2020). Unsplash (https://unsplash.com/photos/bOhKb8e0Iks). In the public domain.

page 95:
From Miroshnichenko, T. (2021). Pexels (https://www.pexels.com/photo/woman-in-white-jacket-holding-mobile-phone-8376168/). In the public domain.

page 96:
From viarami. (2020). Pixabay (https://pixabay.com/images/id-5243199/). In the public domain.

page 99:
From Burival, Z. (2018). Unsplash (https://unsplash.com/photos/V4ZYJZJ3W4M). In the public domain.

page 100:
From Антон Дмитриев. (2020). Unsplash (https://unsplash.com/photos/Q3WVbAfdOoY). In the public domain.

page 103:
From PublicDomainPictures. (2012). Pixabay (https://pixabay.com/images/id-20765/). In the public domain.

page 106:
From tiburi. (2016). Pixabay (https://pixabay.com/images/id-1576418/). In the public domain.

page 108:
From Kusuma, A. (2019). Unsplash (https://unsplash.com/photos/aMl7QzpzYdA). In the public domain.

page 112:
From Salvador, J. (2020). Unsplash (https://unsplash.com/photos/uPrHxo5cPhU). In the public domain.

page 113:
From Reardan, J. (2018). Unsplash (https://unsplash.com/photos/gyslVZcsNK4). In the public domain.

page 118:
From Pixabay. (2016). Pexels (https://www.pexels.com/photo/blur-bright-business-codes-207580/). In the public domain.

page 119:
From cottonbro. (2020). Pexels (https://www.pexels.com/photo/close-up-photo-of-putting-of-fingerprint-on-paper-8382599/). In the public domain.

page 127:
From Element5 Digital. (2016). Unsplash (https://unsplash.com/photos/T9CXBZLUvic). In the public domain.

page 129:
From Dantès, E. (2021). Pexels (https://www.pexels.com/photo/a-peron-filling-up-a-voting-ballot-7103204/). In the public domain.

page 135:
From cottonbro. (2020). Pexels (https://www.pexels.com/photo/boy-in-white-shirt-sitting-on-chair-4709293/). In the public domain.

page 137:
From Winstead, T. (2021). Pexels (https://www.pexels.com/photo/conceptual-photo-of-a-money-scam-7111619/). In the public domain.

page 140:
From Peters, L. (2021). Unsplash (https://unsplash.com/photos/B6JINerWMz0). In the public domain.

page 141:
From Field Engineer. (2017). Pexels (https://www.pexels.com/photo/serious-ethnic-field-engineer-examining-hardware-and-working-on-laptop-442152/). In the public domain.

page 143:
From Burlaka, R. (2016). Pexels (https://www.pexels.com/photo/black-and-gray-photo-of-person-in-front-of-computer-monitor-140945/). In the public domain.

page 145:
From afra32. (2018). Pixabay (https://pixabay.com/images/id-3850511/) In the public domain

page 154:
From Miroshnichenko, T. (2020). Pexels (https://www.pexels.com/photo/person-using-a-computer-5380590/). In the public domain.

REFERENCES

ABS-CBN News. (2020a, March 20). *List: Medical groups that offer online, phone consultations to decongest hospitals amid COVID-19*. https://news.abs-cbn.com/news/03/20/20/list-medical-groups-that-offer-online-phone-consultations-to-decongest-hospitals-amid-covid-19

ABS-CBN News. (2020b, November 27). *E-commerce seen driving PH Internet economy to $28 billion by 2025: Google*. https://news.abs-cbn.com/business/11/27/20/e-commerce-seen-driving-ph-internet-economy-to-28-billion-by-2025-google

Afifa, L. (2021, July 29). *BRI Life customer data breach caused by hacking activity*. Tempo. Co. https://en.tempo.co/read/1488824/bri-life-customer-data-breach-caused-by-hacking-activity

Agcaoili, L. (2020, September 27). BSP backs integrated bills payment facility. *The Philippine Star*. https://www.philstar.com/business/2020/09/27/2045299/bsp-backs-integrated-bills-payment-facility

Al Jazeera. (2020, May 26). *No school until coronavirus vaccine is available: Duterte.* https://www.aljazeera.com/news/2020/5/26/no-school-until-coronavirus-vaccine-is-available-duterte

Albert, J. R. G., Quimba, F. M. A., Tabuga, A. D., Mirandilla-Santos, M. G., Rosellon, M. A., Vizmanos, J. F. V., Cabaero, C. C., & Muñoz, M. S. (2021). *Expanded data analysis and policy research for National ICT Household Survey 2019*. Philippine Institute for Development Studies. https://dict.gov.ph/ictstatistics/wp-content/uploads/2021/08/NICTHS-EDAPR.pdf

Alikpala, R. B. & Ilagan, C. A. (2018, Sep). *A policy brief on the Philippine Water Sector* (Policy Brief No. 7). Arangkada Philippines. http://www.investphilippines.info/arangkada/wp-content/uploads/2015/09/A-Water-Policy-Brief-on-the-Philippines-July2018-SEPT8.pdf

Android Security Bulletin. (2019, Jul). *Android security bulletin—July 2019*. https://source.android.com/security/bulletin/2019-07-01

Anjani, N. H. (2021). *Cybersecurity protection in Indonesia. South Jakarta* [Policy brief]. Center for Indonesian Policy Studies. https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_30f0713c838c4d2a88b8c419838b695f.pdf

Apple Newsroom. (2020, April 11). *Apple and Google partner on COVID-19 contact tracing technology.* https://www.apple.com/au/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Arcilla, J. (2020, June 20). Online classes just one option, DepEd says. *The Manila Times*. https://www.manilatimes.net/2020/06/20/news/top-stories/online-classes-just-one-option-deped-says/733038

Asia Pacific Computer Emergency Response Team. (2019). *APCERT Annual Report 2019*. https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf

Asian Development Bank. (2013). *Philippines: Water supply and sanitation sector assessment, strategy, and road map.* https://www.adb.org/sites/default/files/institutional-document/33810/files/philippines-water-supply-sector-assessment.pdf

Aten, J. (2019, October 9). *Remote working isn't the same as "working from home." Here's the difference and why it matters to your business*. Inc. https://www.inc.com/jason-aten/remote-working-isnt-same-as-working-from-home-heres-difference-why-it-matters-to-your-business.html

Aufa, A. N. (2018). Critical analysis of a technology-based enterprise: A case study of Yahoo! *The International Journal of Applied Business, 2*(1), 39–49. https://www.e-journal.unair.ac.id/TIJAB/article/viewFile/12088/6959

Australian Competition and Consumer Commission. (2020). *Targeting Scams 2019: A review of scam activity since 2009.* https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf

Australian Cyber Security Centre. (n.d.) Critical infrastructure. https://www.cyber.gov.au/acsc/large-organisations-and-infrastructure/critical-infrastructure

Australian Cyber Security Centre. (2021a, June 29). *Joint Cyber Security Centres*. https://www.cyber.gov.au/acsc/view-all-content/programs/joint-cyber-security-centres

Australian Cyber Security Centre. (2021b, September 15). *ACSC Annual Cyber Threat Report 2020–21*. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Australian Government. (2021, September 14). *Australia and Indonesia sign an expanded MoU on Cyber and Emerging Cyber Technology Cooperation.* https://www.internationalcybertech.gov.au/Australia-and-Indonesia-sign-MoU

Australian Signals Directorate. (n.d.). *Cyber security.* https://www.asd.gov.au/cyber

Austria, I., Ignacio, A., Yu, W., & Mirandilla-Santos, G. (2020). *Learning from home: How Philippine schools can respond to the COVID-19 outbreak* [Facebook note]. Facebook. https://www.facebook.com/notes/381262523025716/

Avertium. (2019, March 13). *Crimeware as a service explained*. https://www.avertium.com/blog/crimeware-as-a-service-explained

Ayson, J. (2011, September 8). Hooked Part 5: Off to Cebu—The first contact. *The Ayson Chronicles*. https://jimayson.wordpress.com/2011/09/08/hooked-part-5-off-to-cebu/

Bagram, G., & Ben-Israel, I. (2019). The academic reserve: Israel's fast track to high-tech success. *Israel Studies Review, 34*(2), 75–91.

Bagumbayan-VNP v. COMELEC, G.R. No. 222731 (2016).

Bailey, T., Maruyama, A., & Wallace, D. (2020, November 3). *The energy-sector threat: How to address cybersecurity vulnerabilities*. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Bangko Sentral ng Pilipinas. (2020a). *BSP Digital Payments Transformation Roadmap 2020–2023*. https://www.bsp.gov.ph/Media_And_Research/Primers%20Faqs/Digital%20Payments%20Transformation%20Roadmap%20Report.pdf

Bangko Sentral ng Pilipinas. (2020b). *instaPay FAQ sheet.* https://www.bsp.gov.ph/PaymentAndSettlement/FAQ_Instapay.pdf

Bangko Sentral ng Pilipinas. (2020c). *PESONet FAQ pamphlet.* https://www.bsp.gov.ph/PaymentAndSettlement/FAQ_PESONet.pdf

Bangko Sentral ng Pilipinas. (2020d, August 19). *BSP issuances*. Memorandum No. M-2020-066. https://www.bsp.gov.ph/SitePages/Regulations/RegulationDisp.aspx?ItemId=4369

Belcic, I., & Farrier, E. (2021, September 3). *What is spoofing and how can you prevent it?* Avast Academy. https://www.avast.com/c-spoofing

Bencsáth, B., Pék, G., Buttyán, L., & Felegyhazi, M. (2012). The cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet, 4*(4), 971–1003. https://www.mdpi.com/1999-5903/4/4/971/pdf

Ben-Gurion University of the Negev. (2013). *Ben-Gurion Advanced Technologies Park*. https://in.bgu.ac.il/en/Pages/atp.aspx

Bergemann, K. (2002). A digital free trade zone and necessarily-regulated self-governance for electronic commerce: World Trade Organization, international law, and classical liberalism in cyberspace. *Journal of Computer & Information Law, 20*(4). https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1146&context=jitpl

Bernardo, J. (2020, June 18). *PUP, FEU student portals hacked.* ABS-CBN News. https://news.abs-cbn.com/news/06/18/20/pup-investigating-reports-of-compromised-student-portal

Bertrand, N., & Wolff, E. (2020, December 17). *Nuclear weapons agency breached amid massive cyber onslaught*. Politico. https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855

Better than Cash Alliance. (n.d.). *How to define digital payments?* https://www.betterthancash.org/define-digital-payments

Bisson, D. (2019, July 16). *Telegram, WhatsApp vulnerability exposes media files to tampering*. Security Intelligence. https://securityintelligence.com/news/telegram-whatsapp-vulnerability-exposes-media-files-to-tampering/

Blue, V. (2012, December 9). *WCIT-12 leak shows Russia, China, others seek to define "government-controlled Internet."* ZDNet. https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010). C*ybersecurity governance: A component of MITRE's Cyber Prep Methodology*. MITRE. https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

Borchert, O., Lee, K., Sriram. K., Montgomery, D., Glecihmann, P., & Adalier, M. (2021, September). *BGP secure routing extension (BGP-SRx): Reference implementation and test tools for emerging BGP security standards* (NIST Technical Note 2060). National Institute for Standards and Technology. https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2060.pdf

Bosse, C. M. (2020, December 8). *Stuxnet and beyond: The origins of SCADA and vulnerabilities to critical infrastructure*. GTSC Homeland Security Today. https://www.hstoday.us/subject-matter-areas/infrastructure-security/stuxnet-and-beyond-the-origins-of-scada-and-vulnerabilities-to-critical-infrastructure/

Boubaker, K. (2020, November 16). *Water infrastructure: When states and cyber attacks rear their ugly heads.* Stormshield. https://www.stormshield.com/news/water-infrastructure-when-states-and-cyber-attacks-rear-their-ugly-heads/

Bronk, C. (2014). *Hacks on gas: Energy, cybersecurity, and U.S. defense.* James A. Baker III Institute for Public Policy, Rice University. http://assets.fiercemarkets.net/public/sites/energy/reports/bakerpolicyreport1.pdf

Bureau of Customs. (2021). *Customer Care Portal*. https://client.customs.gov.ph/

Bureau of Fisheries and Aquatic Resources. (2013). *Classified airports.* Geospatial Information System. https://www.bfar.da.gov.ph/files/img/photos/classifiedairports.pdf

Business Australia. (2020). Why your business is at risk from cybersecurity threats: Interview with Shannon Sedgwick. https://www.businessaustralia.com/how-we-help/be-a-better-employer/managing-risk/why-your-business-is-at-risk-from-cyber-security

Butcher, N., Kanwar, A., & Uvalic-Trumbic, S. (2015). *A basic guide to open educational resources*. United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000215804

Cahiles-Magkilat, B. (2020, Jun 22). BPO firm recruiting thousands of WFH jobs. *Manila Bulletin*. https://mb.com.ph/2020/06/22/bpo-firm-recruiting-thousands-of-wfh-jobs/

Campos, O. (2020, May 14). 58% of BPO employees now work at home. *Manila Standard*. https://manilastandard.net/business/it-telecom/323733/58-of-bpo-employees-now-work-at-home.html

Cayon, M. (2020, June 9). Online fraud in PHL worsened during pandemic. *Business Mirror*. https://businessmirror.com.ph/2020/06/09/online-fraud-in-phl-worsened-during-pandemic/

Cervantes, F. (2020a, November 18). *House panel okays funding for dep't of water resources* *bill.* Philippine News Agency. https://www.pna.gov.ph/articles/1122185

Cervantes, F. (2020b, November 24). *House approves Internet transactions bill on final reading.* Philippine News Agency. https://www.pna.gov.ph/articles/1122848

Chairil, T. (2019, May 9). *Cybersecurity for Indonesia: What needs to be done?* The Conversation. https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009

Chairil, T. (2019, September 4). *Indonesia needs to fix "authoritarian" clauses in bill on cyber security before passing it into law.* The Conversation. https://theconversation.com/indonesia-needs-to-fix-authoritarian-clauses-in-bill-on-cyber-security-before-passing-it-into-law-122342

Chandra, G. N. (2021, August 31). Gov't launches investigation after data of 1.3m reportedly leaked from its COVID-19 tracking app. *Jakarta Globe*. https://jakartaglobe.id/tech/govt-launches-investigation-after-data-of-13m-reportedly-leaked-from-its-covid19-tracking-app

Chandra, S., & Shenoy, K. (2016). Cloud networks. In S. Murugesan, & I. Bojanova (Eds.), *Encyclopedia of cloud computing* (pp. 115–127). John Wiley & Sons.

Chandrasekaran, K., & Ananth, A. (2016). Cloud services and service providers. In S. Murugesan, & I. Bojanova (Eds.), *Encyclopedia of cloud computing* (pp. 17–28). John Wiley & Sons.

Chipiongian, L. C. (2021, May 1). Share of digital payments increases to 17%—BSP. *Manila Bulletin*. https://mb.com.ph/2021/05/01/share-of-digital-payments-increasesto-17-bsp/

Christine, D., & Thinyane, M. (2020). *Cyber resilience in Asia-Pacific: A review of national cybersecurity strategies.* United Nations University, Institute of Macau. http://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf

Chuan, T. K. (2020). *The rise and evolution of ransomware during COVID-19*. KPMG. https://home.kpmg/my/en/home/insights/2020/03/the-business-implications-of-coronavirus/the-rise-and-evolution-of-ransomware-during-c-19.html

Cimpanu, C. (2020a, January 19). *Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices.* ZDNet. https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/

Cimpanu, C. (2020b, July 10). *Backdoor accounts discovered in 29 FTTH devices from Chinese vendor C-Data.* ZDNet. https://www.zdnet.com/article/backdoor-accounts-discovered-in-29-ftth-devices-from-chinese-vendor-c-data/

Cimpanu, C. (2020c, July 20). *Two more cyber-attacks hit Israel's water system.* ZDNet. Retrieved September 9, 2021, from https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

Cimpanu, C. (2020d, December 10). *Hackers hide web skimmer inside a website's CSS files.*

ZDNet. https://www.zdnet.com/article/hackers-hide-web-skimmer-inside-a-websites-css-files/

Cisco. (n.d.). *What is a VPN? Virtual private network*. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Citrix. (n.d.). *What is BYOD (Bring Your Own Device)?* https://www.citrix.com/solutions/unified-endpoint-management/what-is-byod.html

Civil Service Commission. (2020). *Amendment to the Revised Interim Guidelines for Alternative Work Arrangements and Support Mechanisms for Workers in the Government During the Period of State of National Emergency Due to COVID-19 Pandemic*. Memorandum Circular No. 18, s. 2020. http://www.csc.gov.ph/phocadownload/MC2020/MC18/MC%20No.%2018,%20s.%202020.pdf

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal of the American Water, 109*(2), 50–58. https://doi.org/10.5942/jawwa.2017.109.0021

Clayton, B., & Segal, A. (2013). *Addressing cyber threats to oil and gas suppliers.* Council on Foreign Relations. https://www.cfr.org/report/addressing-cyber-threats-oil-and-gas-suppliers

Cloudflare (n.d.-a). *What is data privacy?* https://www.cloudflare.com/learning/privacy/what-is-data-privacy/

Cloudflare (n.d.-b). *What is DNS? How DNS works*. https://www.cloudflare.com/learning/dns/what-is-dns/

Cloudflare (n.d.-c) *What is the Internet Protocol?* https://www.cloudflare.com/learning/network-layer/internet-protocol/

CNN Philippines. (2019, September 2). *PSA: Public registration for national ID system to start by July 2020*. https://www.cnnphilippines.com/news/2019/9/2/national-ID-system-public-registration.html

Collier, K. (2020, September 29). *Major hospital system hit with cyberattack, potentially largest in U.S. history.* ABC News. Retrieved September 9, 2021, from https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

Commission of the European Communities. (2005). *Green paper on a European programme for critical infrastructure protection*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN

Commission on Audit. (n.d.). *COA Citizens' Desk Reporting System*. https://cdrs.coa.gov.ph/

Commission on Audit. (2015, October 22). *Prescribing the Government Accounting Manual for use of all national government agencies*. Circular 2015-007. https://www.coa.gov.ph/phocadownloadpap/userupload/Issuances/Circulars/circ2015/COA_C2015-007.pdf

Commission on Elections, Philippine Statistics Authority, & Legal Network for Truthful Elections. (2019). *2019 national and local elections random manual audit.* https://comelec.gov.ph/php-tpls-attachments/2019NLE/Resolutions/mr190893_attachments.pdf

Common Sense. (2019). *2019 state of EdTech privacy report*. https://privacy.commonsense.org/content/resource/state-of-edtech-2019/cs-2019-state-of-edtech-privacy-report.pdf

Commonwealth of Australia. (2009). *Cyber security strategy.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf

Const. (1987), art. III, § 7 (Phil.).

Corera, G. (2020, May 5). *Coronavirus: Cyber-spies hunt COVID-19 research, US and UK warn.* BBC News. https://www.bbc.com/news/technology-52551023

Council of Europe. (n.d.). *The Budapest Convention*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2021). *Chart of signatures and ratifications of Treaty 185—Convention on Cybercrime*. Retrieved May 10, 2021, from https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Counter-Terrorism Committee Executive Directorate. (2017). *Physical protection of critical infrastructure against terrorist attacks.* United Nations Security Council. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf

Cybercrime Prevention Act of 2012, Rep. Act 10175 (2012). https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Cybersecurity and Infrastructure Security Agency. (2020). *Critical infrastructure sectors*. Retrieved January 15, 2021 from https://www.cisa.gov/critical-infrastructure-sectors

Cyber and Infrastructure Security Centre. (2021, August 31). *What is the Cyber and Infrastructure Security Centre.* https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre

Cyber Security Agency. (2016). *Singapore's cybersecurity strategy.* https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/~/media/0ecd8f671af2447890ec046409a62bc7.ashx

Cyber Security Agency. (2022). *Cybersecurity Act—Frequently Asked Questions*. Retrieved February 28, 2022 from https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx#TOPIC_210883

Data Privacy Act of 2012, Rep. Act 10173 (2012). https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

Data Privacy Council Education Sector. (2020). *Data privacy and online learning* (Advisory No. 2020-1). National Privacy Commission. https://www.privacy.gov.ph/wp-content/uploads/2020/10/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf

de Vera, B. O. (2020, June 18). National ID target: 5M heads of poor families by fourth quarter. *Inquirer*. https://business.inquirer.net/300260/national-id-target-5m-heads-of-poor-families-by-fourth-quarter

Department of Defence (Australia). (2000). *Defence 2000: Future defence force.* https://www.defence.gov.au/publications/wpaper2000.PDF

Department of Defense (U.S.). (2018). Summary: Cyber Strategy 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Education (Philippines). (2020, July 1). *DepEd prepares self-learning modules for education's new normal* [Press release]. https://www.deped.gov.ph/2020/07/02/deped-prepares-self-learning-modules-for-educations-new-normal/

Department of Education (U.S.). (2017, January). *Reimagining the role of technology in education*. https://tech.ed.gov/files/2017/01/NETP17.pdf

Department of Energy. (2004). Creation of the DOE Committee for the Security of Critical Infrastructures. *Department Order No. 2004-03-002*. https://www.doe.gov.ph/sites/default/files/pdf/issuances/do_2004-03-002.pdf?withshield=1

Department of Energy. (2021). *Philippine Energy Plan 2020–2040: Towards a sustainable and clean energy future.* https://www.doe.gov.ph/sites/default/files/pdf/pep/pep_2020-2040_signed.pdf

Department of Foreign Affairs and Trade. (n.d.). Ambassador for Cyber Affairs and Critical Technology. https://www.dfat.gov.au/about-us/our-people/homs/ambassador-for-cyber-affairs

Department of Home Affairs. (2016). *Australia's cyber security strategy.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Department of Home Affairs. (2020a, August 6). *Australia's Cyber Security Strategy 2020.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Department of Home Affairs. (2020b). *Critical infrastructure resilience*. Retrieved February 28, 2022 from https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience

Department of Homeland Security. (2009). *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/publication/nipp-2009-partnering-enhance-protection-resiliency

Department of Homeland Security. (2020, January 4). *Summary of terrorism threat to the*

U.S. homeland. National Terrorism Advisory System Bulletin. https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-4-2020

Department of Industry, Science, Energy, and Resources. (2018). *Australia's tech future—Government initiatives.* https://www.industry.gov.au/data-and-publications/australias-tech-future/government-initiatives

Department of Information and Communications Technology. (2017a). *National Cybersecurity Plan 2022.* https://dict.gov.ph/wp-content/uploads/2019/07/NCSP2022-rev01Jul2019.pdf

Department of Information and Communications Technology. (2017b). *Prescribing the policies, rules and regulations on the protection of critical Infrastructure (CII) stipulated in the National Cybersecurity Plan (NCSP) 2022*. Memorandum Circular No. 005. https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-005.pdf

Department of Information and Communications Technology. (2019). *National ICT Household Survey 2019*. ICT Knowledge Portal. https://dict.gov.ph/ictstatistics/nicths2019/

Department of Information and Communications Technology. (2020). *Supplementing the DICT Memorandum Circular Nos. 005, 006, and 007, Series of 2017, and policies, rules and regulations on the implementation of the National Cybersecurity Plan 2022*. Memorandum Circular No. 003. https://dict.gov.ph/wp-content/uploads/2020/03/Dept-Circular-No-003-3062020.pdf

Department of Public Works and Highways. (2019). *Philippine national road network: Brief history and analysis*. 2019 DPWH Atlas. https://www.dpwh.gov.ph/dpwh/2019%20DPWH%20ATLAS/06%20Road%20WriteUp%202019.pdf

Department of the Prime Minister and Cabinet (Australia). (2012). *Annual Report 2011–12*. https://www.pmc.gov.au/sites/default/files/publications/annual_report_11_12.pdf

Department of the Prime Minister and Cabinet (New Zealand). (2019). *New Zealand's Cyber Security Strategy 2019*. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019

Department of State. (2021). *The clean network*. https://2017-2021.state.gov/the-clean-network/index.html

Department of Trade and Industry. (n.d.). *BNRS next gen*. Business Name Registration System. https://bnrs.dti.gov.ph/about

Department of Trade and Industry. (2021). *The basics: E-commerce defined*. DTI Basta E-commerce Madali. https://ecommerce.dti.gov.ph/madali/thebasics.html

Devanesan, J. (2020, July 27). *The Philippines is going cashless—finally.* Techwire Asia. https://techwireasia.com/2020/07/digital-payments-are-finally-soaring-in-the-philippines/

Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998). https://www.

congress.gov/105/plaws/publ304/PLAW-105publ304.pdf

Dimarucut, C. (2019, May 20). *Risk and cybersecurity for critical infrastructure.* SGV. https://www.sgv.ph/c-suite/risk-and-cybersecurity-for-critical-infrastructure

Diokno, B. E. (2019, October 11). *Inclusion and digital transformation—A collaborative approach to regulating fintech.* Retrieved October 9, 2021, from https://www.bis.org/review/r191023g.pdf

Dov, N. (2021, January 5). *2020 was a record year for Israel's security startup ecosystem*. Tech Crunch. Retrieved September 9, 2021, from https://techcrunch.com/2021/01/04/2020-was-a-record-year-for-israels-security-startup-ecosystem/?guccounter=1

Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview* [White paper]. Future of the Internet Initiative, World Economic Forum. https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Draper, P. (2020, January 7). How social engineering is changing the insider threat game. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/opinions/social-engineering-insider-threat/

Duterte, R. (2020, July 27). Fifth State of the Nation Address, July 27, 2020 [Speech transcript]. *The Official Gazette.* https://www.officialgazette.gov.ph/2020/07/27/rodrigo-roa-duterte-fifth-state-of-the-nation-address-july-27-2020/

Dutton, P. (2020, October 20). *New Industry Advisory Committee to support the delivery of national cyber security priorities* [Press release]. Minister for Home Affairs. https://minister.homeaffairs.gov.au/peterdutton/Pages/new-industry-advisory-committee-to-support-national-cyber-security-priorities.aspx

Ease of Doing Business and Efficient Government Service Delivery Act of 2018, Rep. Act 11032 (2018). https://www.officialgazette.gov.ph/downloads/2018/05may/20180528-RA-11032-RRD.pdf

EECSP Expert Group. (2017). *Cyber security in the energy sector: Recommendations for the European Commission on a European strategic framework and potential future legislative acts for the energy sector.* Energy Expert Cyber Security Platform. https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

e-Governance Academy Foundation. (2020, March 6). *National Cyber Security Index*. Retrieved September 9, 2021, from https://ncsi.ega.ee/ncsi-index/

Endo, J. (2020, July 19). Digital payment grows in Philippines amid COVID-19 fears. *Nikkei Asia*. Retrieved from https://asia.nikkei.com/Business/Companies/Digital-payment-grows-in-Philippines-amid-COVID-19-fears

Esguerra, D. (2020, April 14). National ID system could have made cash aid distribution faster—Duterte. *Inquirer*. https://newsinfo.inquirer.net/1258144/national-id-system-could-have-made-cash-aid-distribution-faster-duterte

Esmael, L. K. (2020, May 13). Phishing attacks in PH soar 158% in Q1—Kaspersky. *The Manila Times*. https://www.manilatimes.net/2020/05/13/business/business-top/phishing-attacks-in-ph-soar-158-in-q1-kaspersky/724554

Estrin, D. (2017, February 4). In Israel, teaching kids cyber skills is a national mission. *The Times of Israel*. Retrieved September 9, 2021, from https://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/

European Banking Authority. (2015, March 6). *Technical advice on the delegated acts on critical functions and core business lines*. EBA/Op/2015/05. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/983359/941a6d64-d2f6-44c9-b78e-d0eaca2ca754/EBA-Op-2015-05%20Technical%20Advice%20on%20critical%20functions%20and%20core%20business%20%20%20%20.pdf?retry=1

European Commission. (2020). *eHealth Network: Interoperability guidelines for approved contact tracing mobile applications in the EU*. https://ec.europa.eu/health/sites/default/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

European Union. (1995, January 17). Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications. O.J. (C329). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104

European Union. (2008). On the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. *Council Directive 2008/114/EC*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

European Union Agency for Cybersecurity. (2020). *Procurement guidelines for cybersecurity in hospitals*. https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Eurosmart. (2019, July). *The European Cybersecurity Act*. https://www.eurosmart.com/wp-content/uploads/2019/07/CyberAct_analysis.pdf

Everington, K. (2019, November 26). China can pull plug on Philippines power supply at any time: Report. *Taiwan News*. https://www.taiwannews.com.tw/en/news/3825172

Facebook & Bain & Company. (2020, August 6). *Digital consumers of tomorrow, here today*. https://www.facebook.com/business/news/digital-consumers-of-tomorrow-here-today

Fassihi, F., & Bergman, R. (2021, November 27). Israel and Iran broaden cyberwar to attack civilian targets. *The New York Times*. https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html

Federal Trade Commission. (n.d.). *How to recognize and avoid phishing scams*. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Fidler, D. P. (2020, December 2). *President Trump's legacy on cyberspace policy*. Council on Foreign Relations. Retrieved September 9, 2021, from https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy

FireEye Inc. (2014). *Threat landscape: Retail industry.* https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/retail-campaign.pdf

Fok, E. (2013). An introduction to cybersecurity issues in modern transportation systems. *ITE Journal, 83*(7), 18–21.

Food and Agriculture Organization AIMS (n.d.). Information and communication technologies (ICT). Food and Agriculture Organization of the United Nations. http://aims.fao.org/information-and-communication-technologies-ict

Frei, J. (2020). *Israel's national cybersecurity and cyberdefense posture* (Cyberdefense Report). Center for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Frischmann, B. (2001). Privatization and commercialization of the Internet: Rethinking market intervention into government and government intervention into the market. *The Columbia Science and Technology Law Review, 2*, 1–70. https://journals.library.columbia.edu/index.php/stlr/article/download/3537/1406

Fritchen, K. (2019, November 14). *4 steps to managing EdTech security risks*. Security Boulevard. https://securityboulevard.com/2019/11/4-steps-to-managing-edtech-security-risks/

Frost & Sullivan. (2018). *Understanding the cybersecurity threat landscape in Asia Pacific: Securing the modern enterprise in a digital world*. Microsoft. https://news.microsoft.com/apac/features/cybersecurity-in-asia/

Fruhlinger, J. (2018, August 30). *What is WannaCry ransomware, how does it infect, and who was responsible?* CSO. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Fruhlinger, J. (2020a, June 19). *Ransomware explained: How it works and how to remove it*. CSO. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Fruhlinger, J. (2020b, September 4). *What is phishing? How this cyber attack works and how to prevent it*. CSO. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Fuchs, E. R. (2010). Rethinking the role of the state in technology development: DARPA and the case for embedded network governance. *Research Policy, 39*(9), 1133–1147. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1545155

Garry, A. (2019, July 17). Phishing in K–12: How to avoid taking the bait. *EdTech Magazine*. https://edtechmagazine.com/k12/article/2019/07/phishing-k-12-how-avoid-taking-bait

Gatefy. (2021, April 13). Security statistics and facts that prove email is the main vector of cyber threats. https://gatefy.com/blog/security-statistics-facts-email-main-vector-cyber-threats/

Ghebreyesus, E. (2020, June 4). *Why NHS, UK healthcare orgs need to boost their security in age of COVID-19*. Tripwire. https://www.tripwire.com/state-of-security/healthcare/nhs-uk-healthcare-orgs-boost-security-covid-19/

Gierow, H. (2014). Cyber security in China: New political leadership focuses on boosting national security. *China Monitor, 20*, 1–9. Retrieved September 24, 2021, from http://www.bdo3c.f-sc.org/archives/915.pdf

Glang, H., & Ramos, R. (2015, June 17). *Philippines: Abu Sayyaf again attacks water supply*. Anadolu Agency. https://www.aa.com.tr/en/world/philippines-abu-sayyaf-again-attacks-water-supply/35334

Gold, J. (2020). *The Five Eyes and offensive cyber capabilities: Building a "cyber deterrence initiative."* NATO CCDCOE. https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf

Gonzales, C. (2020a, May 4). CHED: Only 20% of SUCs equipped to facilitate online classes. *Inquirer*. https://newsinfo.inquirer.net/1269090/ched-only-20-of-sucs-equipped-to-facilitate-online-classes

Gonzales, C. (2020b, December 8). Technical issues in cashless toll collection are "birth pains"—NLEX Corp. *Inquirer*. https://newsinfo.inquirer.net/1369270/technical-issues-in-cashless-toll-collection-are-birth-pains-nlex-corp

Google, Temasek, & Bain & Company. (2020). *e-Conomy SEA 2020.* https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf

Google, Temasek, & Bain & Company. (2021). *e-Conomy SEA 2021. Roaring 20s: The SEA digital decade—Indonesia*. https://services.google.com/fh/files/misc/indonesia_e_conomy_sea_2021_report.pdf

Goosen, R. (2017). *Building inclusive digital payments ecosystems: Guidance note for governments*. Report by the Better than Cash Alliance for the G20 Global Partnership for Financial Inclusion, Prepared for the German G20 Presidency. https://www.gpfi.org/sites/gpfi/files/documents/GPFI%20Guidance%20Note%20Building%20Inclusive%20Dig%20Payments%20Ecosystems%20final_0.pdf

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research, 11*(4), 517–525.

Goudos, S. K. (2017). A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic web and applications. *Wireless Personal Communications, 97*(2), 1645–1675.

GOV.PH. (n.d.). *What is the GOV.PH*? https://www.gov.ph/es/about-govph.html

Greenberg, A. (2019, July 7). Hacker lexicon: What is credential dumping? *Wired*. https://www.wired.com/story/hacker-lexicon-credential-dumping/

Greenberg, A. (2021, February 8). A hacker tried to poison a Florida city's water supply, officials say. *Wired*. https://www.wired.com/story/oldsmar-florida-water-utility-hack/

Griffiths, J. (2019, November 26). *China can shut off the Philippines' power grid at any time, leaked report warns.* CNN. https://edition.cnn.com/2019/11/25/asia/philippines-china-power-grid-intl-hnk/index.html

Gross, A., & Murgia, M. (2020, March 28). China and Huawei propose reinvention of the Internet. *Financial Times*. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

Gross, G. (2018, September 28). *Push for greater control over the internet coming back around.* Internet Society. https://www.internetsociety.org/blog/2018/09/push-for-greater-control-over-the-Internet-coming-back-around/

Harris, B. A. (1998). *Firewalls and virtual private networks.* University of Canterbury Repository. https://ir.canterbury.ac.nz/handle/10092/9379

Haydari, A., & Yilmaz, Y. (2018). Real-time detection and mitigation of DDoS attacks in intelligent transportation systems. *21st International Conference on Intelligent Transportation Systems (ITSC)* (pp. 157–163). IEEE.

Iannacci, N. (2018, December 18). *Katz v. United States: The Fourth Amendment adapts to new technology.* Constitution Daily. https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology/

Iasiello, E. J. (2017). Russia's improved information operations: from Georgia to Crimea. *The US Army War College Quarterly*: *Parameters*, *47*(2), 7.

IBM (n.d.-a). *Machine learning*. https://www.ibm.com/cloud/learn/machine-learning

IBM (n.d.-b). *What is digital transformation?* https://www.ibm.com/topics/digital-transformation

IBM Cloud Learn Hub (2020, June 3). *Artificial intelligence (AI)*. IBM. https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

iGov Philippines. (n.d.). *About us*. https://i.gov.ph/about-us/

Information Commissioner's Office. (2020). *COVID-19 contact tracing: Data protection expectations on app development.* https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf

Inter-Agency Task Force on Emerging Infectious Diseases. (2020, April 22). *Recommendations relative to the management of the Coronavirus Disease 2019 (COVID-19) situation*. IATF Resolution No. 27. https://officialgazette.gov.ph/downloads/2020/04apr/20200422-IATF-RESOLUTION-NO-27-RRD.pdf

International Criminal Police Organization. (2020a, April 4). *Cybercriminals targeting critical healthcare institutions with ransomware*. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

International Criminal Police Organization. (2020b, August 4). *Interpol report shows* *alarming rate of cyberattacks during COVID-19*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

International Criminal Police Organization. (2021, January 22). *Interpol report charts top cyberthreats in Southeast Asia*. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

International Telecommunications Union. (2012). *WCIT 2012—Signatories of the final acts.* https://www.itu.int/osg/wcit-12/highlights/signatories.html

International Telecommunications Union. (2019). *Global Cybersecurity Index (GCI) 2018.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Trade Administration (n.d.) *What is eCommerce?* U.S. Department of Commerce. https://www.trade.gov/ecommerce-definitions

Internet Policy Task Force. (2011). *Cybersecurity, innovation and the Internet economy.* Department of Commerce–Internet Policy Task Force. https://www.nist.gov/system/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

Inquirer. (2021, May 9). Dysfunction and disarray [Editorial]. https://opinion.inquirer.net/140058/dysfunction-and-disarray

Jaffee, L. (2020, July 15). Fake Cisco switches provoked network failures. *SC Magazine*. Retrieved from https://www.scmagazine.com/news/security-news/fake-cisco-switches-provoked-network-failures

Jakarta Globe. (2021, May 21). Social security data breach exposes virtually all Indonesians to digital fraud risks. https://jakartaglobe.id/tech/social-security-data-breach-exposes-virtually-all-indonesians-to-digital-fraud-risks

Jaymalin, M. (2020, April 30). *ECQ may prompt review of work-from-home arrangements in Phl.* One News. Retrieved from https://www.onenews.ph/articles/ecq-may-prompt-review-of-work-from-home-arrangements-in-phl

Jercich, K. (2020, May 19). *To "do no harm" invest in cybersecurity.* Healthcare IT News. https://www.healthcareitnews.com/news/do-no-harm-invest-cybersecurity

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupa, C. (2016, October). *Guide to cyber threat information sharing* (NIST Special Publication 800-150). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Jun, Z. (2020, September 7). *China's rapid shift to a digital economy.* Project Syndicate. Retrieved October 19, 2021, from https://www.project-syndicate.org/commentary/china-digital-economy-transformation-pandemic-by-zhang-jun-2020-09

Kan, M. (2020, Jul 21). 7 VPN services found recording user logs, despite “no-lo” pledge. *PC Mag.* https://sea.pcmag.com/encryption-products/38253/7-vpn-services-found-recording-user-logs-despite-no-log-pledge

Kaspersky (n.d.). *What is the deep and dark web?* https://www.kaspersky.com/resource-center/threats/deep-web

Katz v. United States, 389 U.S. 347 (1967). https://caselaw.findlaw.com/us-supreme-court/389/347.html

Keane, S. (2021, September 30). *Huawei ban timeline: Detained CFO makes deal with US Justice Department.* CNET. Retrieved October 1, 2021, from https://www.cnet.com/news/huawei-ban-full-timeline-us-restrictions-china-trump-android-google-ban-antitrust/

Keith, M. (2021, November 27). *Australia will introduce legislation requiring social media companies to reveal anonymous users who post defamatory comments*. Insider. https://www.businessinsider.com/australia-legislation-social-media-companies-reveal-anonymous-trolls-2021-11

Kemp, S. (2021, February 11). *Digital 2021: The Philippines*. Datareportal. https://datareportal.com/reports/digital-2021-philippines

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet computer worm: Harbinger of an emerging warfare capability.* Congressional Research Service. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf

Kindervag, J. (2016, Mar 23). *No more chewy centers: The zero trust model*. Forrester. http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf

Klimburg, A. (2012). *National cyber security framework manual.* NATO CCDCOE. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Kobrata, D., & Atika, R. (2021, November 5). *The privacy, data protection and cybersecurity law review: Indonesia*. The Law Reviews. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/indonesia

Kushner, D. (2013, February 26). *The real story of Stuxnet.* IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

Lakshmanan, R. (2020, April 30). New Android malware steals banking passwords, private data and keystrokes. *The Hacker News*. https://thehackernews.com/2020/04/android-banking-keylogger.html

Lamb, K. (2019, March 19). Indonesia election mired in claims of foreign hacking and “ghost” voters. *The Guardian.* https://www.theguardian.com/world/2019/mar/19/indonesia-election-mired-in-claims-of-foreign-hacking-and-ghost-voters

Lamiel, C. (2017, November 12). *PH government plans to replace textbooks with tablets*. Yugatech. https://www.yugatech.com/news/ph-government-plans-to-replace-textbooks-with-tablets/

Lapowsky, I. (2017, September 8). Facebook may have more Russian troll farms to worry about. *Wired*. https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/

Latto, N. (2021, August 25). *Worm vs. virus: What's the difference and does it matter?* Retrieved September 15, 2021, from Avast. https://www.avast.com/c-worm-vs-virus

Layton, R. (2020, September 4). State Department's 5G clean network club gains members quickly. *Forbes*. Retrieved from https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/?sh=220a93b47536

Lazarte, M. (2016, October 14). *No trust in world without standards*. ISO News. https://www.iso.org/news/2016/10/Ref2128.html

Legal Information Institute. (n.d.). *Expectation of privacy*. Retrieved September 9, 2021, from Cornell Law School. https://www.law.cornell.edu/wex/expectation_of_privacy

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. S. (1997, February 1). The past and future history of the Internet. *Communications of the ACM, 40*(2), pp. 102–108. https://doi.org/10.1145/253671.253741

Lepido, D. (2019, April 30). Vodafone found hidden backdoors in Huawei equipment. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

Lewis, J. A. (2020). Risk, resilience, and retaliation: American perspectives on international cybersecurity. In *Handbook of international cybersecurity* (pp. 252–259). Routledge.

Lilly, B., & Cheravitch, J. (2020). The past, present, and future of Russia's cyber strategy and forces. In T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.) *2020 12th International Conference on Cyber Conflict*. NATO CCDCOE. https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

Lipton, E., Sanger, D. E., & Shane, S. (2016, December 13). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times*. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Lopez, M. (2020, May 7). *Online bank transfers up 25%, ATM transactions down amid pandemic—BSP.* CNN Philippines. Retrieved from https://www.cnnphilippines.com/business/2020/5/7/online-bank-transfers-up-coronavirus.html

Lucas, D. L. (2020, September 8). NBI collars Nigerians suspected in P167-M UCPB cyberheist in Sucat condo raids. *Inquirer*. Retrieved from https://newsinfo.inquirer.net/1332980/nbi-collars-nigerians-suspected-in-p167-m-ucpb-cyberheist-in-sucat-condo-raids

Lukasik, S. J. (2010). Why the ARPANET was built. *IEEE Annals of the History of Computing,* *33*(3), 4–21. https://ieeexplore.ieee.org/document/5432117

Lyons, K. (2020a, June 14). *Germany says its coronavirus contact tracing app is ready.* The Verge. https://www.theverge.com/2020/6/14/21290874/germany-contact-tracing-coronavirus

Lyons, K. (2020b, April 16). *Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week*. The Verge. https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

Lysenko, V., & Brooks, C. (2018, May). Russian information troops, disinformation, and democracy. *First Monday, 23*(5–7), https://doi.org/10.5210/fm.v22i5.8176

Macapagal-Arroyo, G. (2001). Providing for the fourteen pillars of policy and action of the government against terrorism. Memorandum Order No. 37. https://www.officialgazette.gov.ph/2001/10/12/memorandum-order-no-37-s-2001/

Macapagal, M. (2020, August 4). *Scammers tinatarget ang GCash account ng SAP beneficiaries; DSWD nagbababala [Scammers target GCash account of SAP beneficiaries; DSWD warns]*. ABS-CBN News. https://news.abs-cbn.com/news/08/04/20/scammers-tinatarget-ang-gcash-account-ng-sap-beneficiaries-dswd-nagbababala

Malipot, M. H. (2020, October 8). DepEd promotes proper online behavior among students, teachers. *Manila Bulletin*. Retrieved from https://mb.com.ph/2020/10/08/deped-promotes-proper-online-behavior-among-students-teachers/

Manuel, P. (2021, May 21). *BSP eyes full operation of national QR code standard by second half of 2021*. CNN Philippines. https://cnnphilippines.com/business/2021/5/21/BSP-QR-Ph-second-half-2021.html

Marco, B., Liang, C., Yun, G., & Abdullah, I. (2018). *Brunei Cybersecurity Masterplan 2018.* S. Rajaratnam School of International Studies. https://www.researchgate.net/publication/330321721_Brunei_Cybersecurity_Masterplan_2018

Martin, A. J. (2018, July 11). *Russian hackers targeted Ukraine's water supply, security service claims*. Sky News. https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826

Massally, K., Ricart, R., Bambawale, M., Totapally, S., & Bhandari, V. (2019, December). *The state of digital payments in the Philippines.* BSP. https://responsiblefinanceforum.org/wp-content/uploads/2020/02/The_State_of_Digital_Payments_in_the_Philippines-Feb20.pdf

McAfee. (n.d.). *What is malware?* https://www.mcafee.com/en-ph/antivirus/malware.html

MCC Industrial Sales v. Ssangyong Corp, G.R. No. 170633 (October 17, 2007).

McFadden, C. (2021, February 17). *A very brief history of Amazon: The everything store*. Interesting Engineering. https://interestingengineering.com/a-very-brief-history-of-amazon-the-everything-store

Medgate Philippines. (2018, August 22). *Data privacy policy*. https://medgatephilippines.com/dataprivacypolicy.aspx

Medina, A. F. (2020, January 28). *Indonesia's Palapa Ring: Bringing connectivity to the archipelago*. ASEAN Briefing. https://www.aseanbriefing.com/news/indonesias-palapa-ring-bringing-connectivity-archipelago/

Merces, F. (2021). *Ransomware operators found using new "franchise" business model.* Trend Micro. https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

Microsoft. (n.d.). *What is a cloud service provider?* Azure. https://azure.microsoft.com/en-us/overview/what-is-a-cloud-provider/

Microsoft. (2020, April 28). *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk*. Microsoft 365 Defender Threat Intelligence Team. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Microsoft. (2021, October 14). *Azure Identity Management and access control security best practices*. Azure. https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Migration and Home Affairs (n.d.). *Critical infrastructure*. European Commission. https://ec.europa.eu/home-affairs/pages/page/critical-infrastructure_en

Miyao, Y. (2016, Dec 12). *Image-borne malware: How viewing an image can infect a device*. OPSWAT. https://www.opswat.com/blog/image-borne-malware-how-viewing-image-can-infect-device

Mockapetris, P. V., & Dunlap, K. J. (1988). Development of the Domain Name System. *SIGCOMM '88: Symposium Proceedings on Communications Architectures and Protocols* (pp. 123–133). Association for Computing Machinery. https://doi.org/10.1145/52324.52338

Mogato, A. (2019, April 26). *El Niño damage to agriculture now at P7.96 billion—DA*. Rappler. https://www.rappler.com/business/el-nino-damage-agriculture-as-of-april-25-2019

Montemayor, M. (2020, July 21). *21.7M learners enrolled for incoming school year: DepEd*. Philippine News Agency. https://www.pna.gov.ph/articles/1109587

Morais, A., & Obar, J. (2018). Mobile Internet. In B. Warf (Ed.), *The SAGE encyclopedia of the Internet* (Vol. 1, pp. 645–648). SAGE.

Morales, N., & Lema, K. (2016, December 9). *Philippines outsourcing firms hit by Trump and "Trump East."* Reuters. Retrieved from https://www.reuters.com/article/us-usa-trump-philippines-idUSKBN13X2Q6

Mueller, R.S., III. (2019). *Report on the investigation into Russian interference in the 2016 presidential election.* U.S. Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download

Mühlberg, B. (2020, April 22). FCC urged to consider China telecom a national security threat. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/fcc-urged-to-consider-china-telecom-a-national-security-threat/

Mulyadi, & Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment national cyber and crypto agency (BSSN). *2018 6th International Conference on Cyber and IT Service Management (CITSM)*. IEEE. https://doi.org/10.1109/CITSM.2018.8674265

Muncaster, P. (2018, September 18). FBI warns parents of EdTech security risk. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/fbi-warns-parents-of-edtech/

Mylrea, M. (2017). Smart energy-Internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. *The Journal of World Energy Law & Business, 10*(2), 147–158.

Nadeau, M. (2021, May 6). *Cryptojacking explained: How to prevent, detect, and recover from it*. CSO. https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

Nakashima, E., & Harris, S. (2018, July 13). How the Russians hacked the DNC and passed its emails to WikiLeaks. *The Washington Post*. Retrieved September 9, 2021, from https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

NAPOCOR v. Codilla, G.R. No. 170491 (Apr. 4, 2007).

Nation, J. (2018, April 25). *Major DNS spoofing hack affects Amazon Web Services*. Metacert. https://medium.com/metacert/major-dns-spoofing-hack-affects-amazon-web-services-157e3565c844

National Cyber Directorate. (2017). *Israel national cyber security in brief*. Prime Minister's Office. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf

National Cyber Security Agency. (2020). *Malaysia Cybersecurity Strategy 2020–2024*. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

National Cyber Security Agency. (2022). *The critical national information infrastructure*. Retrieved March 1, 2022 from https://www.nacsa.gov.my/cnii.php

National Economic Development Authority. (2020, June 1). *E-commerce seen to sustain PH economy and drive growth*. https://neda.gov.ph/e-commerce-seen-to-sustain-ph-economy-and-drive-growth/

National Institute of Standards and Technology. (n.d.). *Critical infrastructure*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/critical_infrastructure

National Institute of Standards and Technology. (2006, March). *Minimum security* *requirements for federal information and information systems* (FIPS PUB 200. Federal Information Processing Standards Publication). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

National Institute of Standards and Technology. (2012, September). *Guide for conducting risk assessments: Information security* (NIST Special Publication 800-30 Revision 1). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2015, December). *Supplemental information for the interagency report on strategic U.S. government engagement in international standardization to achieve U.S. objectives for Cybersecurity* (NISTIR 8074 Volume 2). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

National Institute of Standards and Technology. (2018a, August 12). *Cybersecurity framework: The five functions*. Retrieved September 9, 2021, from https://www.nist.gov/cyberframework/online-learning/five-functions

National Institute of Standards and Technology. (2018b, April 16). *Framework for improving critical infrastructure cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2020, May 21). *NIST and COVID-19.* https://www.nist.gov/coronavirus

National Institutes of Health. (n.d.). *National Telehealth Center*. University of the Philippines Manila. https://nih.upm.edu.ph/institute/national-telehealth-center

National People's Congress. (2017). Promulgated by the Standing Committee of the 12th National People's Congress, adopted June 27, 2017. https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

National Privacy Commission. (2020a, July 8). *Guidelines for establishments on the proper handling of customer and visitor information for contact tracing* (NPC PHE Bulletin No. 15). https://www.privacy.gov.ph/2020/07/npc-phe-bulletin-no-15-guidelines-for-establishments-on-the-proper-handling-of-customer-and-visitor-information-for-contact-tracing/

National Privacy Commission. (2020b, October 1). *Privacy dos and don'ts for online learning in public K-12 classes* (NPC PHE Bulletin No. 16). https://www.privacy.gov.ph/2020/10/npc-phe-bulletin-no-16-privacy-dos-and-donts-for-online-learning-in-public-k-12-classes/

National Security Council. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure.* https://irp.fas.org/eprint/cyber-review.pdf

National Security Office. (2019, April). *National cybersecurity strategy.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

Newton, D. (2015, November 4). Cheating in online classes is now big business. *The Atlantic*. Retrieved from https://www.theatlantic.com/education/archive/2015/11/cheating-through-online-courses/413770/

Norton (n.d.). *What is antivirus software? Antivirus definition*. https://us.norton.com/internetsecurity-malware-what-is-antivirus.html

Noruzi, A. (2004). Introduction to Webology. *Webology.* https://www.webology.org/2004/v1n1/a1.html

NTT Application Security. (n.d.). *Information leakage: Application security terminology*. https://www.whitehatsec.com/glossary/content/information-leakage

Obama, B. (2015). *Remarks by the president at the cybersecurity and consumer protection summit* [Speech transcript]. Office of the Press Secretary, The White House. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation. (2021, April 24). *Gov't issues Presidential Regulation 28/2021 on National Cyber and Encryption Agency (BSSN)*. https://setkab.go.id/en/presidential-regulation-28-2021-on-national-cyber-and-encryption-agency-bssn/

Office of Management and Budget. (2017, January 3). *Memorandum for heads of executive departments and agencies* (M-17-12). Executive Office of the President. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf

O'Flaherty, K. (2020, July 29). New Netflix threat: This legit-looking scam could steal your credit card details. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2020/07/29/new-netflix-threat-this-legit-looking-scam-could-steal-your-credit-card-details/?sh=52ce7a2869d2

Olmstead v. United States, 277 U.S. 438 (1928). https://caselaw.findlaw.com/us-supreme-court/277/438.html

Opall-Rome, B. (2015, June 25). Israel confirms it was cyber attack target. *Defense News*. Retrieved September 9, 2021, from https://www.defensenews.com/2015/06/24/israel-confirms-it-was-cyber-attack-target/

Osisanya, S. (n.d.). National security vs global security. *UN Chronicle*. United Nations. https://www.un.org/en/chronicle/article/national-security-versus-global-security

Palli, I. C. (2020, April 22). *WHO, Gates Foundation credentials dumped online: Report*. BankInfoSecurity. https://www.bankinfosecurity.com/who-gates-foundation-credentials-dumped-online-report-a-14167

Palmer, D. (2021, January 21). *Ransomware victims that have backups are paying ransoms to stop hackers leaking their stolen data.* ZDNet. https://www.zdnet.com/article/ransomware-victims-that-have-backups-are-paying-ransoms-to-stop-hackers-leaking-their-stolen-data/

Palmer, D. (2021, May 14). *Learning from cyberattacks could be the key to stopping them.* ZDNet. https://www.zdnet.com/article/learning-from-cyber-attacks-could-be-the-key-to-stopping-them/

Parliament of Australia. (2018). *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

Patdu, I. (2020, March 19). *Privacy should not be an obstacle to telemedicine.* Newsbytes.PH. https://newsbytes.ph/2020/03/19/patdu-privacy-should-not-be-an-obstacle-to-telemedicine/

Patdu, I. D., & Tenorio, A. S. (2016). Establishing the legal framework of telehealth in the Philippines. *Acta Medica Philippina, 50*(4), 237–346.

Patrizio, A. (2017, June 8). *British Airways' outage, like most data center outages, was caused by humans.* Network World. https://www.networkworld.com/article/3200105/british-airways-outage-like-most-data-center-outages-was-caused-by-humans.html

Payne, M. (2021, April 21). *Launch of Australia's International Cyber and Critical Technology Engagement Strategy*. Minister for Foreign Affairs. https://www.foreignminister.gov.au/minister/marise-payne/media-release/launch-australias-international-cyber-and-critical-technology-engagement-strategy

Penn, A. (2020, May 6). *Safer online and the new normal.* Telstra News. https://exchange.telstra.com.au/safer-online-and-the-new-normal/

People v. Enojas, G.R. No. 204894 (Mar. 10, 2014).

Peters, J. (2020, April 2). *Automated tool can find 100 Zoom meeting IDs per hour.* The Verge. https://www.theverge.com/2020/4/2/21206061/zoom-meeting-id-zwardial-automated-tool

Pex, J. (n.d.) *Exemption from IDF service—Legal information*. Cohen, Decker, Pex & Brosh. https://lawoffice.org.il/en/exemption-from-idf-service/

Pfeifer, S., Fildes, N., & Ram, A. (2018, April 7). Energy sector on alert for cyber attacks on UK power network. *Financial Times*. https://www.ft.com/content/d2b2aaec-4252-11e8-93cf-67ac3a6482fd

Philippine Statistics Authority. (n.d.). *Philippine Identification System (PhilSys)*. http://rsso04a.psa.gov.ph/philsys/faqs

Philippine Statistics Authority. (2018). *Implementing rules and regulations of Republic Act 11055*. https://psa.gov.ph/system/files/kmcd/IRR%20of%20the%20RA%2011055%20or%20PhilSys%20Law.pdf

Philippine Statistics Authority. (2020a). *PhilSys operations in light of COVID-19*. https://psa.gov.ph/press-releases/id/161102

Philippine Statistics Authority. (2020b). *PhilSyS project information memorandum: System* *integrator*. https://psa.gov.ph/content/philippine-identification-system-philsys-project-information-memorandum-systems-integrator

Philippine Statistics Authority. (2021a). PhilSyS online step 1 registration now at 4 million successful registrants. https://psa.gov.ph/content/philsys-online-step-1-registration-now-4-million-successful-registrants

Philippine Statistics Authority. (2021b). PhilSyS registers 50 million Filipinos; hits target for 2021. https://psa.gov.ph/content/philsys-registers-50-million-filipinos-hits-target-2021

PhilSys Act, Rep. Act 11055. (2018). https://www.officialgazette.gov.ph/downloads/2018/08aug/20180806-RA-11055-RRD.pdf

PHP.Net. (n.d.). *What is PHP?* https://www.php.net/manual/en/intro-whatis.php

Pilette, C. (2021, July 26). *What is social engineering? A definition + techniques to watch for*. Norton–Emerging Threats. https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

Pinandita, A. (2020, May 23). Calls mount for comprehensive audit into data breach affecting 2.3 million voters. *The Jakarta Post*. https://www.thejakartapost.com/news/2020/05/22/calls-mount-for-comprehensive-audit-into-data-breach-affecting-2-3-million-voters.html

Pizzi, M. (2014, January 7). *Cyberwarfare greater threat to US than terrorism, say security experts*. Al Jazeera America. Retrieved September 9, 2021, from http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html

Porcalla, D. (2020, November 10). DTI: Online scams rose 500 percent this year. *Philstar*. https://www.philstar.com/headlines/2020/11/10/2055751/dti-online-scams-rose-500-percent-year

Press, G. (2017, July 18). 6 reasons Israel became a cybersecurity powerhouse leading the $82 billion industry. *Forbes*. Retrieved September 9, 2021, from https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=b1951ba420aa

Prime Minister's Office. (2020, June 19). *Statement on malicious cyber activity against Australian networks.* Office of the Prime Minister of Australia. https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

Privacy International. (n.d.). *Five Eyes*. https://privacyinternational.org/learn/five-eyes

Public Safety Canada. (2018). *National Cyber Security Strategy: Canada's vision for security and prosperity in the digital age.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Pursiainen, C. (2021). Russia's critical infrastructure policy: What do we know about it? *European Journal for Security Research, 6*(1), 21–38. https://doi.org/10.1007/s41125-020-00070-0

Rahardjo, B. (2017). The state of cybersecurity in Indonesia. In J. Edwin, & T. Ross, *Digital Indonesia: Connectivity and divergence* (pp. 110–124). ISEAS.

Ramos, C. (2020a, February 4). NGCP violated Constitution for allowing Chinese to hold high position—Senators. *Inquirer*. https://newsinfo.inquirer.net/1223452/ngcp-violated-constitution-by-allowing-chinese-to-hold-high-position-senators

Ramos, C. (2020b, June 30). Duterte: DepEd allocating P700M for Internet connections of 7,000 public schools. *Inquirer*. https://newsinfo.inquirer.net/1299437/duterte-deped-allocating-p700m-for-internet-connections-of-7000-public-schools

Ramos, C. (2020c, September 3). DTI sees 4K percent rise in online businesses during virus lockdown. *Inquirer*. https://business.inquirer.net/306480/dti-sees-4k-percent-rise-in-online-businesses-during-virus-lockdown

Rappler. (2018, November 10). *Over 100,000 Filipinos affected by Cathay Pacific data breach.* https://www.rappler.com/technology/thousands-filipinos-affected-cathay-pacific-data-breach

Raska, M. (2015). *Confronting cybersecurity challenges: Israel's evolving cyber defence strategy.* S. Rajaratnam School of International Studies–Nanyang Technology University. Retrieved September 9, 2021, from https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf

Raywood, D. (2020, November 26). DDoS attacks against online retailers increase four-fold during pandemic. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/ddos-online-four/

Rechtschaffen, D. (2019, June 27). Why China's data regulations are a compliance nightmare for companies. *The Diplomat*. https://thediplomat.com/2019/06/why-chinas-data-regulations-are-a-compliance-nightmare-for-companies

Red Hat (2017, October 31). *What is an API?* https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces

Reuters. (2013, January 25). *U.S. Homeland chief: Cyber 9/11 could happen "imminently."* Retrieved September 9, 2021, from https://www.reuters.com/article/us-usa-cyber-threat-idUSBRE90N1A320130124

Reuters. (2017, May 13). *Two major Indonesian hospitals attacked in "ransomware" storm*. https://www.reuters.com/article/us-cyber-attack-indonesia-idUSKBN1890AX

Reuters. (2019, August 22). *Factbox: Israel a global leader in growing market for cyber weapons*. Retrieved September 9, 2021, from https://www.reuters.com/article/uk-israel-hackers-factbox-idUKKCN1VC0Y8

Reuters, T. (2016, January 11). *Cyberattack that crippled Ukrainian power grid was highly coordinated.* CBC News. https://www.cbc.ca/news/science/ukraine-cyberattack-1.3398492

Rey, A. (2019, April 25). *Cebu Pacific's GetGo server breached.* Rappler. https://www.rappler.

com/technology/cebu-pacific-getgo-server-breach-april-2019

Risk Based Security. (2020). *2020 Q3 report: Data breach quickview*. https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf

Rizal, M., & Yani, Y. M. (2016). Cybersecurity and its implementation in Indonesia. *Journal of ASEAN Studies, 4*(1), 61–79.

Robertson, J., & Riley, M. (2018, October 4). The big hack: How China used a tiny chip to infiltrate US companies. *Bloomberg*. Retrieved September 9, 2021, from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Rodriguez, M. (2019). Disinformation operations aimed at (democratic) elections in the context of public international law: The conduct of the internet research agency during the 2016 US presidential election. *International Journal of Legal Information, 47*(3), 149–197.

Rosenbach, E., & Chong, S. (2019). *Governing cyberspace: State control vs. the multistakeholder model.* Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved September 24, 2021, from https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model

Roth, A. (2021, January 11). Code deployed in US cyber-attack linked to suspected Russian hackers. *The Guardian*. https://www.theguardian.com/world/2021/jan/11/solarwinds-hack-russian-spying-tools-hackers-malware-fsb

Rudd, K. (2008, December 4). *Parliamentary debates: House of Representatives National Security speech* [Speech transcript]. Parliament of Australia. https://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2008-12-04/0045/hansard_frag.pdf;fileType=application%2Fpdf

Salazar, M. (2020, April 29). *BPOs in PH adjust to new remote work arrangements, new technologies.* Backend News. https://backendnews.net/bpos-in-ph-adjust-to-new-remote-work-arrangements-new-technologies/

Samaniego, A. (2020, November 14). How hackers collected sensitive data from the Land Transportation Office. *Manila Bulletin*. https://mb.com.ph/2020/11/14/how-hackers-collected-sensitive-data-from-the-land-transportation-office/

Samarati, P., & di Vimercati, S. (2016). Cloud security: Issues and concerns. In S. Murugesan, & I. Bojanova (Eds.), *Encyclopedia of cloud computing* (pp. 207–219). John Wiley & Sons.

Samosir, G. (2020, August). *Can Indonesia achieve "100 Smart Cities" by 2045?* [White paper]. YCP Solidiance. https://ycpsolidiance.com/white-paper/can-indonesia-achieve-100-smart-cities-by-2045

Sanger, D. E., & Perlroth, N. (2019, June 15). U.S. escalates online attacks on Russia's power grid. *The New York Times*. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (Source behind paywall)

Santiago, J. (2015, July 22). *Top countries best prepared against cyberattacks.* World Economic Forum. https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/

Saputra, P., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's cyber security through public–private partnership (PPP). *Central European Journal of International & Security Studies, 13*(4), 104–120.

Schlesinger, J., & Solomon, R. (2020, January 31). *A cyberattack known as e-skimming is getting more common with the rise of online shopping.* CNBC. https://www.cnbc.com/2020/01/31/e-skimming-cyberattack-is-growing-along-with-online-shopping.html

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare.* Cambridge University Press.

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D.I. (2008, October). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule: Information security* (NIST Special Publication 800-66 Revision 1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

Schroeder, P. (2020, August 7). *Capital One to pay $80 million fine after data breach*. Reuters. https://www.reuters.com/article/us-usa-banks-capital-one-fin-idUSKCN2522DA

Schwartz, M. (2020, July 27). *Dave: Mobile banking app breach exposes 3 million accounts*. Data Breach Today. https://www.databreachtoday.com/dave-mobile-banking-app-breach-exposes-3-million-accounts-a-14708

Scroxton, A. (2020, June 12). NHS email service users ensnared in phishing attack. *Computer Weekly*. https://www.computerweekly.com/news/252484590/NHS-email-service-users-ensnared-in-phishing-attack

Seals, T. (2016, February 8). Massive brute-force attack on Alibaba affects millions. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/massive-bruteforce-attack-on/

Seals, T. (2020, April 28). *Enterprise security woes explode with home networks in the mix*. Threatpost. https://threatpost.com/enterprise-security-woes-explode-home-networks/155280/

Security Magazine. (2020a, June 2). Lookout report: 37% increase in worldwide in enterprise mobile phishing attacks. https://www.securitymagazine.com/articles/92496-lookout-report-37-increase-in-worldwide-in-enterprise-mobile-phishing-attacks

Security Magazine. (2020b, November 18). Pharmaceutical industry sees increase in mobile phishing encounters. https://www.securitymagazine.com/articles/93963-pharmaceutical-industry-sees-increase-in-mobile-phishing-encounters

Senate of the Philippines. (2020, May 4). *Teleconferencing a go* [Press release]. https://legacy.senate.gov.ph/press_release/2020/0504_prib3.asp

Shalal, A. (2020, April 24). *WTO report says 80 countries limiting exports of face masks, other goods*. Reuters. https://www.reuters.com/article/us-health-coronavirus-trade-wto-idUSKCN2253IX

Sihaloho, M., & Yasmin, N. (2019, September 27). Cybersecurity bill postponed until House's next term. *Jakarta Globe*. https://jakartaglobe.id/context/cybersecurity-bill-postponed-until-houses-next-term/

Singapore Cybersecurity Act. (2018). Singapore Statutes Online. https://sso.agc.gov.sg/Acts-Supp/9-2018/

SOCRadar. (2021). *Threat landscape report—Indonesia*. https://socradar.io/wp-content/uploads/2021/10/2021-Indonesia-Threat-Landscape-Report.pdf

Solomon, S. (2020, December 20). Israeli tech firms raise record $9.93 billion in 2020 but M&A deals plunge. *The Times of Israel*. Retrieved September 9, 2021, from https://www.timesofisrael.com/israeli-tech-firms-raise-record-9-93-billion-in-2020-but-ma-deals-plunge/

Southam, M. (2014, May). DNSSEC: What it is and why it matters. *Network Security, 2014*(5), 12–15. https://doi.org/10.1016/S1353-4858(14)70050-9

Spafford, E. H. (1989). *The Internet worm incident* (Report No. 89-933). Department of Computer Science, Purdue University. https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1792&context=cstech

Specops. (2020, July 9). *The countries experiencing the most "significant" cyber-attacks.* https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

Springer, P. (2017). Cryptography. In *Encyclopedia of cyber warfare* (pp. 38–40). ABC-CLIO.

SSH.com. (2021). *What is PKI (public key infrastructure)?* SSH Academy. https://www.ssh.com/academy/pki

StaySafe.PH. (2020). *Privacy notice*. https://angeles.staysafe.ph/data-privacy

Stilgherrian. (2019a, October 28). *Cyber Security Strategy 2020: Civil society experts slam "national security" agenda*. ZDNet. https://www.zdnet.com/article/cyber-security-strategy-2020-civil-society-experts-slam-national-security-agenda/

Stilgherrian. (2019b, November 25). *Renewed calls for dedicated Australian cyber minister and cyber leadership*. ZDNet. https://www.zdnet.com/article/renewed-calls-for-dedicated-australian-cyber-minister-and-cyber-leadership/

Strom, D. (2021, April 8). *What is IAM? Identity and access management explained.* CSO. https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Stubbs, J., & Bing, C. (2020, May 6). *State-backed hackers targeting coronavirus responders, U.S. and UK warn.* Reuters. https://www.reuters.com/article/us-health-coronavirus-cyber-idUSKBN22H1UG

Stupp, C. (2020, May 14). Hackers change ransomware tactics to exploit coronavirus crisis. *The Wall Street Journal*. https://www.wsj.com/articles/hackers-change-ransomware-tactics-to-exploit-coronavirus-crisis-11589448602

Sullivan, B. (2019, January 11). *FBI warns EdTech needs stronger defenses for students' personal data*. Security Intelligence: https://securityintelligence.com/fbi-warns-edtech-needs-stronger-defenses-for-students-personal-data/

Sumologic. (n.d.). *What is an attack vector?* https://www.sumologic.com/glossary/attack-vector/

Supreme Court of the Philippines. (2020a). *2019 Amendments to the 1989 Revised Rules on Evidence.* A.M. No. 19-08-15-SC. https://sc.judiciary.gov.ph/files/amendments/2019-rules-on-evidence.pdf

Supreme Court of the Philippines. (2020b). *Additional courts authorized for pilot-testing of hearings through videoconferencing*. Office of the Court Administrator Circular 100-2020. https://oca.judiciary.gov.ph/wp-content/uploads/2020/06/OCA-Circular-No.100-2020.pdf

Supreme Court of the Philippines. (2020c). *Courts in areas placed under general community quarantine from 16 to 31 May 2020.* Administrative Circular No. 40-2020. https://sc.judiciary.gov.ph/11371/

Supreme Court of the Philippines. (2020d). *Implementation of Supreme Court Administrative Circular No. 33-2020 on the electronic filing of criminal complaints and informations, and posting of bails*. Office of the Court Administrator Circular 89-2020. https://oca.judiciary.gov.ph/wp-content/uploads/2020/06/OCA-Circular-No.-89-2020.pdf

Supreme Court of the Philippines. (2020e). *Modified enhanced community quarantine in certain areas until 31 May 2020.* Administrative Circular No. 39-2020. https://sc.judiciary.gov.ph/11362/

Supreme Court of the Philippines. (2020f). *Online filing of complaint or information and posting of bail due to the rising cases of COVID-19 infection.* Administrative Circular No. 33-2020. https://sc.judiciary.gov.ph/11145/

Supreme Court of the Philippines. (2020g). *Pilot testing of hearings of criminal cases involving persons deprived of liberty through videoconferencing.* Administrative Circular No. 37-2020. https://sc.judiciary.gov.ph/11249/

Swiss Cyber Forum. (2020). *All you need to know about cyber security threats in energy sector.* https://www.swisscyberforum.com/all-you-need-to-know-about-cyber-security-threats-in-energy-sector

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147–164.

Telecommunication Regulator of Cambodia. (2014). *Summary on Cambodian ICT Masterplan 2020.* https://www.moeys.gov.kh/index.php/en/policies-and-strategies/3887.html#.YffuJvVBwq0

Telecommunications and Information Working Group. (2019). *APEC framework for securing the digital economy.* Asia-Pacific Economic Cooperation. https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy

Tessian. (2020, September 7). Why we click: The psychology behind phishing scams and how to avoid being hacked. https://www.tessian.com/blog/why-we-click-on-phishing-scams/

Tetangco, A. M. (2015, October 27). *Scaling up inroads in financial inclusion for a quantum leap* [Speech transcript]. BIS. https://www.bis.org/review/r151202b.pdf

The Associated Press. (2021, September 21). Indonesia says no evidence of alleged Chinese intel hack. *The Asahi Shimbun*. https://www.asahi.com/ajw/articles/14444857

The Daily Telegraph. (2019, October 14). Chalmers says cyber hits cost the economy $29 billion a year. https://www.dailytelegraph.com.au/news/national/chalmers-says-cyber-hits-cost-the-economy-29-billion-a-year/video/a1ad39ad5995c6ae9f2eece4cfec5fe5

The Jakarta Post. (2017, May 15). Ransomware attacks nation's largest cancer hospital. https://www.thejakartapost.com/news/2017/05/15/ransomware-attacks-nations-largest-cancer-hospital.html

The Toronto Star. (2008, August 6). Security hole menaces Web users. https://www.thestar.com/news/world/2008/08/06/security_hole_menaces_web_users.html

The White House. (2011, April). *National strategy for trusted identities in cyberspace: Enhancing online choice, efficiency, security, and privacy.* Homeland Security Digital Library. https://www.hsdl.org/?view&did=7010

The White House. (2018, September). *National cyber strategy of the United States of America*. Trump White House Archives. Retrieved September 9, 2021, from https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Thompson, M. (2016, March 24). Iranian cyber attack on New York dam shows future of war. *Time*. Retrieved from https://time.com/4270728/iran-cyber-attack-dam-fbi/

Tidy, J. (2021, June 16). *Why cyber gangs won't worry about US–Russia talks.* BBC News. https://www.bbc.com/news/technology-57504007

Times of Israel. (2020, October 16). Cybersecurity groups: Iranians targeted top Israeli firms in ransomware attack. Retrieved September 9, 2021, from https://www.timesofisrael.com/cybersecurity-groups-iranians-targeted-top-israeli-firms-in-ransomware-attack/

Torres v. PAGCOR, G.R. No. 193531 (Dec. 14, 2011).

Trend Micro. (n.d.). *Business email compromise (BEC)*. https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

Trend Micro. (2020, November 11). *Developing story: COVID-19 used in malicious campaigns*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Trines, S. (2017, December 10). *Academic fraud, corruption, and implications for credential assessment*. World Educaton News + Reviews. https://wenr.wes.org/2017/12/academic-fraud-corruption-and-implications-for-credential-assessment

Tucker, E. (2018, July 14). 12 Russians indicted for meddling in 2016 US election. *Associated Press News*. Retrieved September 9, 2021, from https://apnews.com/article/1ddb174446a34785becd670275fedcbf

United Nations Institute for Department Research. (2021, June). *Vietnam*. Cyber Policy Portal. https://unidir.org/cpp/en/states/vietnam

United States Senate. (2018). *Report of the Select Committee on Intelligence United States Senate on Russian active measures campaigns and interference in the 2016 U.S. election. Vol. 2: Russia's use of social media with additional views*. 116th Congress. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Uren, T. (2020, November 11). *Australia's Cyber Security Strategy*. RUSI. https://rusi.org/explore-our-research/publications/commentary/australias-cyber-security-strategy

USA Patriot Act of 2001, § 1016 Pub. L. No. 107-56 , 115 Stat. 401 (2001). https://www.congress.gov/bill/107th-congress/house-bill/3162

Valdez, D. A. (2019, May 24). Globe stands firm on Huawei partnership. *Business World*. https://www.bworldonline.com/globe-stands-firm-on-huawei-partnership/

Vavra, S., & Starks, T. (2020, December 18). *How the Russian hacking group Cozy Bear, suspected in the SolarWinds breach, plays the long game*. Cyberscoop. https://www.cyberscoop.com/cozy-bear-apt29-solarwinds-russia-persistent/

Verizon. (2020a). *2020 data breach investigations report*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Verizon. (2020b). *2020 payment security report.* https://enterprise.verizon.com/en-nl/resources/reports/2020/2020-payment-security-report.pdf?cmp=paid_social:beltug:ves_emea_sec_bnlx:PSR:tower_based

Vijayan, J. (2020, April 14). *Pandemic could make schools bigger targets of ransomware attacks.* Dark Reading. https://www.darkreading.com/attacks-breaches/pandemic-could-make-schools-bigger-targets-of-ransomware-attacks

Villanueva, J. (2020, October 8). *BSP says policy governing digital banks out before year-end.* Philippine News Agency. https://newsbytes.ph/2020/10/08/bsp-says-policy-governing-digital-banks-out-before-year-end/

Vodopyan, E. (2022, January 13). *What is data leakage?* Netwrix. https://blog.netwrix.com/2021/02/10/data-leakage/

vpnMentor. (n.d.). *Report: Indonesian government's COVID-19 app accidentally exposes over 1 million people in massive data leak*. https://www.vpnmentor.com/blog/report-ehac-indonesia-leak/

Wagner, J. (2017, June 1). China's cybersecurity law: What you need to know. *The Diplomat*. Retrieved September 24, 2021, from https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

White, M. (2020, July 14). Middle East braces itself for cyber warfare. *Global Trade Review*. Retrieved September 9, 2021, from https://www.gtreview.com/magazine/volume-18-issue-3/middle-east-braces-cyber-warfare/

Whitney, L. (2020, August 20). How the shift to remote working has impacted cybersecurity. *Tech Republic*. https://www.techrepublic.com/article/how-the-shift-to-remote-working-has-impacted-cybersecurity/

WHOA.com. (n.d.). *Databreach 101: Top 5 reasons it happens*. https://www.whoa.com/data-breach-101-top-5-reasons-it-happens/

Widianto, S., & Potkin, F. (2020, May 22). *Indonesia probes breach of data on more than two million voters.* Reuters. https://www.reuters.com/article/us-indonesia-cyber-breach-idUSKBN22Y15K

Woetzel, J., Seong, J., Wang, K., Manyika, J., Chui, M., & Wong, W. (2017, August 3). *China's digital economy: A leading global force.* McKinsey Global Institute. https://www.mckinsey.com/featured-insights/china/chinas-digital-economy-a-leading-global-force

Wolber, J. (2016). Opening a can of worms and viruses: The impact of e-service on e-mail users everywhere. *New York Law School Law Review, 61*(3–4), 449–472. https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1231&context=nyls_law_review

World Bank. (2012). *Broadband strategies handbook*. https://ddtoolkits.worldbankgroup.org/sites/default/files/2018-10/Broadband%20Strategies%20Handbook.pdf

World Health Organization (2010). Telemedicine: Opportunities and developments in member states: Report on the second global survey on eHealth 2009. *Global Observatory for eHealth Series – Volume 2*. https://www.who.int/goe/publications/goe_telemedicine_2010.pdf

World Health Organization. (2020, April 23). *WHO reports fivefold increase in cyber attacks, urges vigilance*. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Yerman, J. (2019, May 22). A startup nation: Why Israel has become the new Silicon Valley. *APEX Experience Magazine*. Retrieved September 9, 2021, from https://apex.aero/articles/startup-nation-israel-become-silicon-valley/

Zetter, K. (2014, November 3). An unprecedented look at stuxnet, the world's first digital weapon. *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zhu, G., Chou, M. C., & Tsai, C. W. (2020). Lessons learned from the COVID-19 pandemic exposing the shortcomings of current supply chain operations: A long-term prescriptive offering. *Sustainability, 12*(14), 5858. https://www.mdpi.com/2071-1050/12/14/5858/pdf

Secure Connections

The Asia Foundation