

CYBERCRIME INVESTIGATION AND COORDINATION CENTER

01000011 01001001 01000011 01000011

NATIONAL CYBERSECURITY PLAN 2022



DICT

NATIONAL CYBERSECURITY PLAN 2022

01110000 01110000 01101100 01111001 00100000 01000011 01101000 01100001 01101001 01101110 01110011
00100000 01001001 01101110 01100100 01101001 01110110 01101001 01100100 01110101 01100001 01101100 01110011

01010000 01110010 01101111 01110100 01100101 01100011 01110100 01101001 01101111 01101110 00100000
01000011 01001001 01001001 00100000 01000111 01101111 01110110 00100111 01110100 00100000 01010011 01110101

MESSAGE



My warmest greetings to the Department of Information and Communications Technology (DICT) on the launching of the National CyberSecurity Plan 2022.

Your department plays a crucial role in the government's efforts to address the challenges brought about by global interconnectivity. I commend the DICT for crafting this Cybersecurity Plan which aims to deal with these challenges and improve our people's confidence in the ICT sector.

May the implementation of this new cybersecurity framework enable you to fulfill your mandate of securing critical ICT infrastructure while ensuring personal data privacy and confidentiality. It is my hope that you will use this framework in realizing your role in nation-building through the creation of a cybersecurity educated society.

I wish you all the best in this endeavor.

A handwritten signature in black ink, appearing to read 'Rodrigo Duterte'.

RODRIGO ROA DUTERTE
President of the Philippines

MESSAGE



The Philippine government has invested in Information and Communications Technology (ICT) infrastructure and applications as the cornerstone for national economic growth. ICT is recognized as key enabler for economic growth and social mobility and is expected to improve the quality of life of people as part of the longterm vision for the Philippines AmbisyonNatin 2040 and the ASEAN Masterplan of 2015. Though there is the promise of acceleration in the nation's growth via the rapid development of ICT in the Philippines, this technology and their applications have introduced new types of threats such as cybercrime, cyber espionage, cyber terrorism and cyber warfare to mention a few. Cyber threats are on the rise, and are sophisticated and difficult to mitigate; the imminent threat of cyber crimes to National

Security necessitates that the government must be prepared and in position to respond and counter adequately these cyber threats.

Given the Philippines' heavy dependence on ICT to support its economic development goals, it is imperative that information infrastructure or "infostructure" among others be resilient, robust, and secure against cyber threats. The National Cybersecurity Plan 2022 was crafted to establish an environment that will assure trust and confidence in everyone while using ICT facilities, and ensure that the Philippines is self-reliant and able to protect its interests, particularly national security. This plan will guarantee the availability of cyber services and the confidentiality and integrity of information processes, assets, and sensitive information of Individuals, Businesses, and Government itself.

Pursuant to RA 10844, the Department of Information and Communications Technology shall ensure the security of critical infostructure including information assets and data of the government, individuals, and businesses. The Department is working in collaboration with key stakeholders in Cybersecurity, especially the Cybercrime Investigation and Coordination Center and the Philippine National Police. As the lead in the formulation of cybersecurity policies, the Department will periodically review their implementation progress to ensure that threats of current and potential cyberattacks are addressed adequately and effectively in a timely and appropriate manner.


RODOLFO A. SALALIMA
Secretary, Department of Information
and Communications Technology (DICT)

MESSAGE



As we become more and more dependent on ICT in our daily lives, an equal responsibility to provide online security should be established. Through the National Cybersecurity Plan, the DICT is providing a roadmap for ICT stakeholders to secure their online environment. It is the government's strategy to safeguard the ICT environment of the country which will prepare and secure the government infostructure, systematically strengthen critical infostructure (CII) for resiliency, use security measures among businesses to protect, prevent, respond, and recover from attacks especially within CII and government supply chains, and raise awareness of cyber risks among users for empowerment in adopting the right norms in Cybersecurity.

Accepting the reality that there is no physical or economic security without cybersecurity, the Department of Information and Communications Technology is now officially enforcing the National Cybersecurity Plan 2022 hereby sending a message that the government is at the forefront of protecting every Filipino in cyberspace.


ELISEO M. RIO, JR.
Undersecretary
Special Concerns

MESSAGE



The constantly changing times and the advent have drastically altered the way we perform our duties and responsibilities. There are certain groups whose ideology is to destroy the order of our nation and are now using advanced and sophisticated technologies to carry out their plans, thus, the need to develop measures in protecting and policing the cyberspace has now become one of the major responsibilities of the DICT to assure the Filipino people of its safe use especially in doing business.

The DICT is mandated to establish cybersecurity measures that would guard the country against cyber threats. The department will be in the frontline to protect Philippines' critical

infrastructure, government and military networks, businesses and supply chains, and the Filipino people through the crafting of a comprehensive and realistic national cybersecurity plans, policies and programs. DICT will enforce, evaluate, and constantly monitor these cybersecurity policies through regular assessment and compliance activities, conduct of annual cyber drills and exercises, and cybersecurity education and awareness programs.

As cyberspace is borderless in nature, international cooperation will be at the highest possible level to curb cyber threats and aid our law enforcement authorities, prosecution services, and cyber defense centers through the establishment of the National Computer Emergency Response Team (NCERT) that would act as the focal entity to achieve a safe and resilient cyber community.

Let us be together in the fight against cyber threats as CyberSecurity is not just a whole of government approach but of the whole Filipino nation.


ALLAN S. CABANLONG
Assistant Secretary for Cybersecurity
and Enabling Technologies, DICT

MESSAGE



I congratulate the Department of Information and Communications Technology (DICT) for crafting the National Cybersecurity Plan (NCSP) 2022.


Online connectivity has been transformed from a luxury and privilege to a necessity for the Filipino people. However, the government has been slow in providing Philippine cyberspace with the proper measures and safeguards that would enable the general public to conduct their businesses and expand their knowledge using online means, without facing security risks. This is why the NSC considers cybersecurity as an important part of national security.

One particular importance of cybersecurity is connected with how the government should deal with security issues on government issued documents. This is because in our interconnected society, the integrity of these documents-which more or less prove our right to be recognized as Filipino citizens-have become terrifyingly vulnerable to malcontents and our identity could be compromised as a result.

Cybersecurity comes in by ensuring that the database would be impervious to cyber attacks and pilferage of data. Ensuring that cybersecurity is in place and addressed by the Philippine government also has implications on our economic security. Other governments and businesses would have more confidence in our processes, businesses, and government if we have more robust and responsive cybersecurity.

In this regard, I look forward to the eventual implementation of the NCSP 2022, as well as to closer cooperation of the NSC and the DICT on matters of mutual concern.

Mabuhay!


HERMOGENES C. ESPERON, JR.
National Security Adviser and
Director-General, NSC

MESSAGE



Our One Defense Team extends warm felicitations to the Department of Information and Communications Technology (DICT) for having formulated this well-crafted National Cybersecurity Plan 2022.

Having set forth the DICT's policy direction within the National Cybersecurity Strategy Framework, this plan shall serve as a guide on how you can best fulfill your mandate of ensuring the privacy and confidentiality of our citizens' personal information; and securing critical ICT infrastructure and information assets of the government, individuals and businesses. It shall also improve your provision of oversight functions to agencies governing and regulating the ICT sector, strengthen consumer protection and welfare, ensure data privacy and

security, and foster completion and growth of the ICT sector.

We cannot overemphasize the urgency of protecting the nation's critical information structures especially government public and military networks, to ensure continuous operations even during crises and emergencies. Thus, we are one with you in instituting measures to enhance our ability to respond to cybersecurity threats before, during, and after attacks.

Rest assured of our efforts to assist the DICT in informing and educating our people on cybersecurity, not only in the workplace but also in our homes, communities, and other places where we access the Internet. This is the first step toward instilling cybersecurity consciousness in every Filipino so that we can all contribute in building a safe, secure, and cyber-resilient nation.

Once more, congratulations to the DICT on the significant accomplishment!

Mabuhay ang Pilipinas! Mabuhay tayong lahat!

DELFIN N. LORENZANA
Secretary, Department of National Defense

MESSAGE



I extend my warm congratulations to the Department of Information and Communications Technology (DICT) on the crafting and publication of the National Cybersecurity Plan 2022.

This Plan is most welcome as it sets the direction in addressing the urgency to protect the nation's critical infrastructure, government networks, business enterprises, corporations and their supply chains, and most of all, every Filipino using the Internet. This publication comes at this most opportune time when information and communications technology is developing

and advancing at a rapid pace and playing an increasingly crucial role in the lives of our countrymen.

I take this opportunity to assure the DICT of the strong support and cooperation of the Philippine National Police (PNP) in the implementation of cybersecurity measures and policies and in continually improving and strengthening the nation's response to the increasing threats to peace and security being posed over cyberspace.

I lead the men and women of the PNP in forging a stronger partnership with the DICT as we endeavor to keep Philippine cyberspace safe and secure.

More power to the DICT! Mabuhay kayo!

RONALD M. DELA ROSA
Police Director General
Chief, Philippine National Police

CONTENTS

| | |
|---|----|
| EXECUTIVE SUMMARY | 02 |
| Introduction | 06 |
| Scope | 08 |
| The Cyber Threat Landscape | 08 |
| Global and Regional Threat Landscape | 10 |
| The Philippine Threat Landscape | 11 |
| Sources of Threats | 13 |
| The National Strategic Context | 16 |
| The National Cybersecurity Plan 2022 | 16 |
| The NSCP 2022 Vision | 17 |
| Strategic Initiatives | 17 |
| The National Cybersecurity Framework | 17 |
| The Guiding Principles | 21 |
| Roles and Responsibilities | 22 |
| Key Areas for Cybersecurity | 25 |
| Classification of National Security System | 28 |
| Risk Management Approach | 29 |
| Strategic Collaboration | 30 |
| Key Strategic Initiatives | 31 |
| Key Program Areas | 32 |
| Protection of Critical Information Infrastructure (CII) | 32 |
| Protection of Government Networks | 35 |
| Protection of Supply Chains | 39 |
| Protection of Individuals | 39 |
| Active Approach | 41 |
| Identify | 41 |
| Protect | 41 |
| Detect | 41 |
| Respond | 41 |
| Recover | 41 |
| Proactive Approach | 41 |
| Defend | 41 |
| Deter | 42 |
| Develop | 42 |
| Metrics | 43 |
| Conclusion | 45 |
| Glossary | 46 |

TABLE OF ABBREVIATIONS

| | |
|-------|---|
| AFP | Armed Forces of the Philippines |
| CICC | Cybercrime Investigation and Coordination Center |
| CII | Critical Infostructure |
| CISO | Chief Information Security Officer |
| DDoS | Distributed Denial of Service |
| DICT | Department of Information and Communications Technology |
| ICT | Information and Communications Technology |
| IoT | Internet of Things |
| ISSP | Information Systems Strategic Plan |
| LEA | Law Enforcement Development Life Cycle |
| NCERT | National Computer Emergency Response Team |
| NCIAC | National Cybersecurity Inter-Agency Committee |
| NCSP | National Cybersecurity Plan |
| NIST | National Institute of Standards and Technology |
| NSC | National Security Council |
| NSS | National Security System |
| NTC | National Telecommunications Commission |
| PDCA | Plan → Do → Check → Act |
| RAT | Remote Access Trojan |
| SWIFT | Society for Worldwide Interbank Financial Communication |

EXECUTIVE SUMMARY

The rapid changes in information and communications technology (ICT) have drastically altered the way we live. There are growing dependencies on these technologies that include critical functions of industries and industry control systems. The newly created Department of Information and Communications Technology, through its attached agency, the Cybercrime Investigation and Coordination Center (CICC), adapts to the new paradigm with the comprehensive National Cybersecurity Strategy Framework.

The development of the Framework shall institutionalize the adoption and implementation of Information Security Governance and Risk Management approaches. These globally recognized standards shall provide the government a systematic and methodical practice of ensuring the protection of our mission critical and non-critical infostructure. The government shall build its capability and capacity for quick response and recovery through the establishment of the National Emergency Response Team (NCERT).

Included in the mandates of DICT are to “ensure the rights of individuals to privacy and confidentiality of their personal information; ensure the security of critical ICT infrastructures including information assets of the government, individuals and businesses; and provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of the ICT sector.”

One of the priority areas that the Department has to immediately institute is the formulation of the National Cybersecurity Plan to address the urgency to protect the nation’s Critical Infostructures, Government Networks both Public and Military, Small Medium Enterprises to Large Businesses and Corporations and its supply chains, and every Filipino using the Internet.

The primary goals of this Plan include: (1) assuring the continuous operation of our nation’s critical infostructure, and public and military networks; (2) implementing cyber resiliency measures to enhance our ability to respond to threats before, during, and after attacks; (3) effective coordination with law enforcement agencies; and (4) a cybersecurity-educated society.

I. Making Critical Information Infrastructure (CII) Trusted and Secure

The functions and services of critical infostructure and those of the governmental bodies are vital to the country’s socio-economic activities. Any interruption of these functions and services can cause direct and significant consequences to people’s safety and security; therefore, it is crucial to take precautionary measures to address potential threats. It is necessary to take “mission assurance”-based approaches. Mission owners should analyze risks and should have discussions with asset owners in order to accomplish the functions and services of critical infostructure or the governmental bodies. Mission owners should ask comprehensive decisions of senior executives by providing information on vulnerabilities including resultant risks.

II. Making Government Information Environment Secure

To respond to cyberattacks, particularly targeted ones that are apparently aimed at stealing, damaging, or altering information, the agency will take government-wide, multi-layered measures based on the assumption of cyberattacks. This must also include contingency plans for this possibility – a certain entity will be used as a springboard for another entity that is the original target of a cyberattack. In promoting these measures, the Government will ensure that they are based on common internationally accepted standards for the governmental bodies, and will conduct risk analysis on its administrative responsibilities to optimize the processes involved in making government information environment secure.

III. Making Businesses Secure

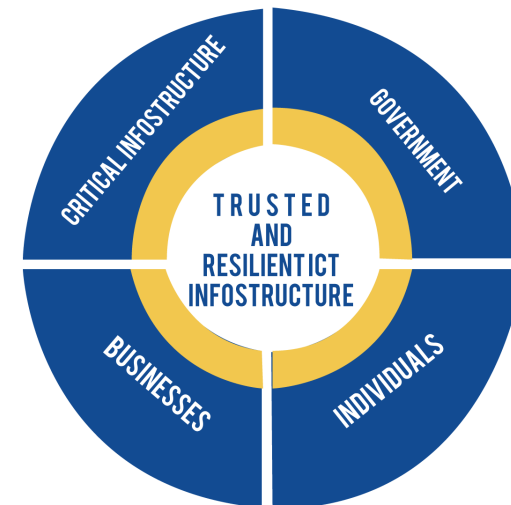
Along with the continuous increased interconnectivity of cyberspace and physical space, the number of cybersecurity incidents closely related to individuals and enterprises – such as illegal money transfers by exploiting Internet banking, stealing information by targeted attacks, and phishing – has drastically grown.

There is also a rise in the number of breaches of personal or confidential information, including a large-scale personal data breach. Thus, such repeated crimes have become serious social concerns. Without advanced cybercrime response and investigative capabilities, it is difficult to capture the reality of malicious cybercrimes; to control cybercrimes appropriately in accordance with laws and statutes; and to be ready to handle new methods of cybercrimes that would likely emerge in the near future.

IV. Making Individuals Aware and Secure

In the current environment, cyber risks have become more complex and diversified and Internet users with insufficient cybersecurity awareness become victims or end up becoming offenders unknowingly.

Therefore, the Internet and the advent of mobile technology have increased utilization of computers, smartphones, and other devices to transact, process, transmit, and store information. The public awareness and knowledge of cybersecurity should reach suf-

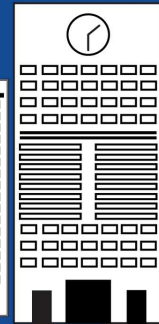
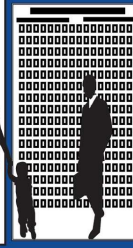
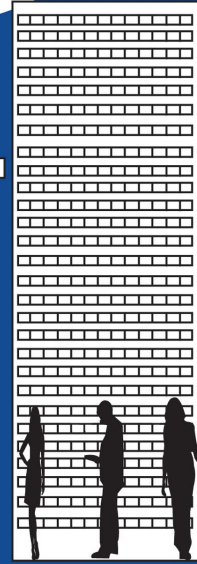
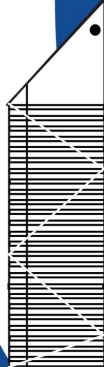
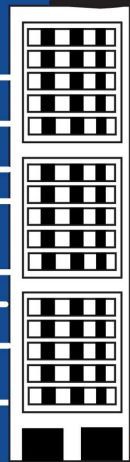


**Making Critical
Information
Infrastructure (CII)
Trusted and Secure
#CyberResilientPH**

**Making Government
Information
Environment Secure
#CyberToughPH**

**Making Individuals Aware
and Secure
#CyberSafePH**

**Making Businesses Secure
#CyberAssurancePH**



INTRODUCTION



The rapid development on Information and Communications Technologies (ICT) created a vast environment for vertical, as well as horizontal challenges and opportunities. Data and information can now travel at the speed of light. The world has become interconnected through supercomputers and massive network systems and the Internet superhighways, in a way that is almost unimaginable. This created cyberspace. The internet has introduced many drastic changes in our lives. This is apparent in the way we process and communicate our information to transact, interact, and connect with other people.

The digitization of our society has also created new sets of paradigms of dependencies and interdependencies. The government has recognized the importance of information and the vital role of information and communications technology as one of the enablers for nation building.

The growing dependencies of the government in ICT to deliver its essential services have brought home the hard facts that we must have a robust and resilient infrastructure. Our computer, information, and network systems must be given priority to ensure that the integrity of our cyberspace is not put in jeopardy as we entrust our data and our information into this virtual environment.

Although there is an implemented government-wide program on Information Systems Strategic Plan (ISSP) which provides the blueprint for planning, developing, building, and/or acquiring technology such as hardware and software applications for each government agency, the design has never incorporated the security aspect on top priority in facilitating the creation of a digital environment. Therefore, individuals with malicious intent are able to discover the gaps between these systems and are able to exploit it.

Making Critical Information Infrastructure (CII) trusted and secure

Making government information environment more secure

Making business more secure

Making individuals aware and secure

Addressing these gaps will mitigate the risks, threats and vulnerabilities from malicious actors such as criminals, terrorist organizations, individuals or even hostile states.

The technological revolution on mobile-based devices and smart systems and the expansion of inter-networking of devices, computing systems, and mechanical and digital machines for connectivity through Internet (also known as Internet of Things or IoT) introduced a whole new host of threats into our cyberspace. As we rely heavily on systems (e.g. banking), technologies (e.g. telecommunications), and infrastructure (e.g. power grids) to conduct the daily activities of our lives which are connected to the internet, these are potentially vulnerable to interference or disruptions.

Recognizing all these issues and challenges that may be a potential threat to our national security and national interest, the National Cybersecurity Plan 2022 has been prepared to address the cyber threats and create innovative measures that will lead to a secure and resilient Philippine cyberspace. In

However, the NCSP 2022 shall provide the institutional framework and foundation where policies and initiatives will be developed, formulated, and prepared.

Just to name a few, we also have several legal instruments such as the Cybercrime Prevention Act, E-Commerce Law, and the Data Privacy Act that provide the mechanisms for enforcing laws and provision of penalties and regulating through policies and guidelines.

Launching on these objectives, the DICT has identified and shall focus its attention on four national targets and make them a national priority.

The scale and dynamic nature of cyber threats mean we need to work harder to develop our capabilities and defenses. A comprehensive approach is required to effectively secure our cyberspace. To have this realized, investments on intervention and measures must be prepared through initial assessment of where we are now and what we have.

SCOPE

The National Cybersecurity Plan 2022 is intended to shape the policy of the government on cybersecurity and the crafting of guidelines that will be adapted down to the smallest unit of the government. The strategy also intends to provide a coherent set of implementation plans, programs, and activities to be shared to the public and the private sector, the civil society, and the academe, including the private individuals.

The strategy covers the entire country including all Philippine networks connected through government networks, domestic and international. The strategy also mandates that all government and public systems shall be assessed and must be classified under the National Security System.

The nexus of the cybersecurity strategy is anchored on the last three clauses under Section 2 of the Republic Act No. 10844, to wit, “(l) to ensure the rights of individual to privacy and confidentiality of their personal information;(m) to ensure the security of the critical ICT infrastructures including information assets of the government, individuals, and businesses; and (n) to provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, and foster competition and growth of the ICT sector.”

Therefore, the context of cybersecurity within this document refers to the protection of information systems (hardware and software including associated and support infrastructure), the data within these systems, and the services that are provided by these systems from any unauthorized access, harm

or misuse, whether it includes intentional or accidental, or from natural disasters.

The above definition is reflective of the definition of cybersecurity¹ from the International Standards on Guidelines for Cybersecurity (ISO/IEC 27032:2012), “preservation of confidentiality, integrity, and availability of information in the Cyberspace”, which incidentally was also adopted from the International Standards on Information Security Management System (ISO/IEC 27000:2014). For the purpose of this document, it shall adopt the definition from ISO/IEC 27032:2012.

Thus, Information Security, Application Security, Network Security, Internet Security, and CII Protection are central to the key areas of developing the cybersecurity plan of the government. The objective of this document is set to share the vision of the Government for cybersecurity in 2022 and the key objectives to achieve the goal, including the guiding principles, roles and responsibilities of all key players and the stakeholders.

THE CYBER THREAT LANDSCAPE

To understand better the threat that we are now facing in the digital age, the black market having a pivotal role in cyber threats is discussed briefly within this section.

The criminal underground operating with the use of the web is highly fragmented. Each organized criminal group offers specialized expertise on certain services and each actively offers said services on the deep web.



A report from Trend Micro² indicated that there are at least six different cybercriminal ecosystems that are actively operating across Europe, North and South America, Africa, and Asia.

Each of these criminal ecosystems offers unique and specialized services in the black market. Stiff competition in the Russian black market pushes up the game. The sellers provide goods in the shortest amount of time, with the most efficiency. The Russian black market is one of the pioneers in the underground economy and provides support to budding counterparts such as Germany.

The Japanese underground on the other hand is still relatively new in the cybercrime economy. It prefers to cater more on taboo rather than on the typical illegal trade that occurs in the black market and is only exclusive to specific members.

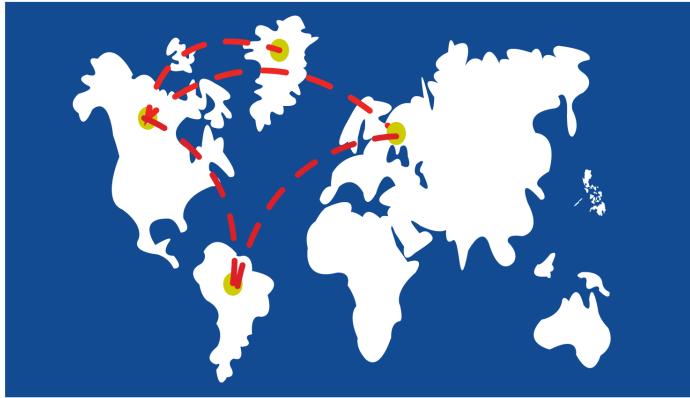
However, as it learns more of the “benefits” anonymity offers, the Japanese underground market now boasts uncommon offerings such as leaked data search engine privacy protection services.

The Chinese underground economy sells both software and services similar to its counterparts. The economy has a robust offering of tools and hardware development and acts as a prototype hub for criminals.

The North American underground encourages novices to jumpstart a career in the criminal world. This type of criminal ecosystem is not exclusive to members like the Japanese and is unlike the tech-savvy hackers like Russians, Germans, and Chinese. Unlike its US counterpart, the Canadian underground prefers to sell fake or stolen documents and credentials.

1 International Organization for Standardization. (2012). Information Technology – Security Techniques – Guidelines for Cybersecurity, 1st Edition. Published in Switzerland.

2 <http://www.trendmicro.fr/media/wp/cyber-crime-and-the-deep-web-whitepaper-en.pdf>



The German underground market functions similar to the Deep Web where it offers various wares and caters to a niche set of customers. Although it is also still relatively new, its Russian counterparts provide them support, such as shared resources and parallel sites as well as cross-market advertising.

For any young criminal aspirant, the Brazilian underground market provides the avenue to reach instant superstardom for notoriety. They mostly focus on banking Trojans. Most of these budding cybercriminals are young and bold enough to flaunt and operate on the “Surface Web” by frequenting popular social media sites. However, they mostly work independently from one another.

GLOBAL AND REGIONAL THREAT LANDSCAPE

This section mentions two most prominent cases in 2015 and 2016 respectively, as an example to emphasize the importance of the Critical Information Infrastructure³ (CII) in our nation. Any attack can erode our trust in the system that we rely heavily on to provide

continuous service without disruptions or interruptions.

On December 23, 2015, a disruptive⁴ cyber-attack on the electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo in Western Ukraine⁵ occurred and caused a major power outage. The region experienced a blackout for several hours affecting more than 220,000 consumers. Upon investigation, six months before the attack, phishing emails were sent to the offices of power utility companies in Ukraine which contains malicious Microsoft Office documents. The malware was able to gather intelligence and managed to obtain credentials that allowed the attackers to gain direct remote control of aspects of the network and open the circuit breakers that subsequently enabled the attacker to trigger the outage.

In February 2016⁶, an attacker was able to access the SWIFT (Society for Worldwide Interbank Financial Communication) payment system of the Bangladesh Bank and instructed the New York Federal Reserve Bank to transfer money from an account in Bangladesh Bank to multiple accounts in the

Philippines. These fraudulent transactions led to a loss of US\$101 million when these were completed and went through the payment and transfer system of the bank. However, the banking system was able to prevent the attempted transactions to defraud an additional US\$850 million. After the discovery of the attack, a forensic investigation was launched and the discovery was made that a malware was installed in the bank’s systems and had been used to gather information on the procedures used by the bank for international payment and fund transfers. Further analysis also indicated that the malware linked to the attack showed a sophisticated functionality for interacting with the local SWIFT Alliance Access software running on the Bangladesh Bank infrastructure. It was concluded that the conduct of the criminals are geared towards more sophisticated attacks on network intrusions.

The Components of Malicious Cyber Activity

In the “Economic Impact of Cyber Crime and Cyber Espionage” report by McAfee, a global computer security software company, the count in estimating losses from cybercrime, cyber espionage, and malicious cyber activity was broken down into six parts

- The loss of intellectual property and business confidential information
- Cybercrime, which costs the world hundreds of millions of dollars every year
- The loss of sensitive business information, including possible stock market manipulation

- Opportunity costs, including service and employment disruptions, and reduced trust for online activities
- The additional cost of securing networks, insurance, and recovery from cyber attacks
- Reputational damage to the hacked company

Put these together and the cost of cybercrime and cyber espionage to the global economy is probably measured in the hundreds of billions of dollars. To put this in perspective, the World Bank says that global GDP was about \$70 trillion in 2011. A \$400 billion loss—the high end of the range of probable costs—would be a fraction of a percent of global income. But this begs several important questions about the full benefit to the acquirers and the damage to the victims from the cumulative effect of cybercrime and cyber espionage⁷.

THE PHILIPPINE THREAT LANDSCAPE

This section of the document provides a background on the early initiatives that the government has undertaken to start establishing security in our cyberspace as well as citing cases of threats and recent breaches into the government system.

The Context of Cybersecurity in the Philippines

The dynamic and fluid changes in the cyber environment make the challenges, risks, and threats more complex. The government is

3 <http://www.gov.ph/2012/09/12/republic-act-no-10175/>

4 <http://www.express.co.uk/news/uk/731832/UK-faces-BLACKOUTS-cyber-hackers-threaten-energy-supplies>

5 <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

6 <http://www.reuters.com/article/us-cyber-bank-ing-swift-exclusive-idUSKCN0XM2DI>

cognizant of these facts and realities of the virtual environment. Information as a critical asset of the government, the public and private sector and down to the individuals that reside within our computer systems, network systems, or application systems must be protected and secured from being compromised or breached. As early as 1965, laws have already been passed to protect people and property and to prosecute individuals or a group of individuals who violate and cause harm to our right to privacy of information or those who seek to compromise our system. To cite a few, we have the Anti-Wire Tapping Act of 1965 and the Electronic Commerce Act of 2000.

In 2004, the Arroyo Administration has included in its priority the agenda of establishing a National Cybersecurity Plan. This became one of the main reference documents when the Information Security

Incident Response Manual was crafted in 2013 through the Information and Communications Technology (ICT) Office.

On September 2015, the Executive Order No. 189 which created the National Cybersecurity Inter-Agency Committee or NCIAC was signed. The creation of the National NCIAC is a necessary undertaking reflective of its vision towards creating a safe Philippine Cyberspace. One of the most important aspects in the creation of the NCIAC is to have one direction in the coordination between government agencies and other relevant sectors. This provides an avenue in building a consensus that requires national attention, and immediate decision and action such as the pre-preparation of appropriate and effective measures to strengthen cybersecurity capabilities against existing and future cyber threats.

To adapt to the fluid state of changes of the information and communications technologies, the Internet and cyberspace, the Philippine Congress passed into law on May 23, 2016 the Republic Act No. 10844 which is The Creation of the DICT.

Under R.A. 10844, it paved the way for a National Agency to focus and address ICT-related issues and matters. Incidentally, the Cybercrime Prevention Act of 2012 (R.A. 10175) which constituted the creation of the Cybercrime Investigation and Coordinating Center (CICC) and the National Privacy Commission which was created through the Data Privacy Act of 2012 (R.A. 10172).

In the creation of the DICT, the National Telecommunications Commission (NTC), the CICC and the NPC were placed under the Department as attached agencies.

of hacking, defacement, and Distributed Denial of Service or DDoS.

The Philippines is no stranger to being a victim of cyber-espionage. A Finland-based security firm reported¹⁰ in 2016, that a malware was found targeting confidential information of government and private organization. The malicious virus called Remote Access Trojan (RAT) is often disguised as an innocent file but once it has been opened, it releases a virus into the victim's computer and gathers intelligence to be sent back to the attacker.

SOURCES OF THREATS

Cyber criminals

There are two interrelated forms of criminal activity that increase the risks of the potential threat against information assets of government, public, and private sectors and trickles down to ordinary individuals:

Cyber-enabled criminals

These are traditional crimes that are perpetuated, magnified, and increased in scale or reach through the use of computers, computer networks, and other forms of Information and Communications Technology or ICT (e.g. cyber-enabled fraud and data theft).

Cyber-dependent criminals

These are crimes that can be committed through the use of ICT devices. These devices become an instrument for both committing the crime and the target of the crime (e.g. hacking to steal data, developing and propagating malware to be used to intrude and breach systems for financial gains, disruptions of network systems, etc.).

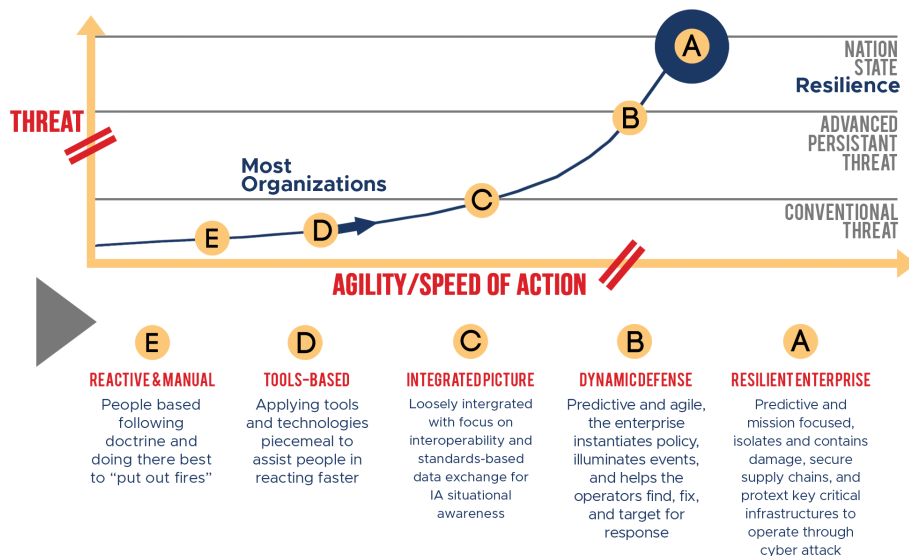


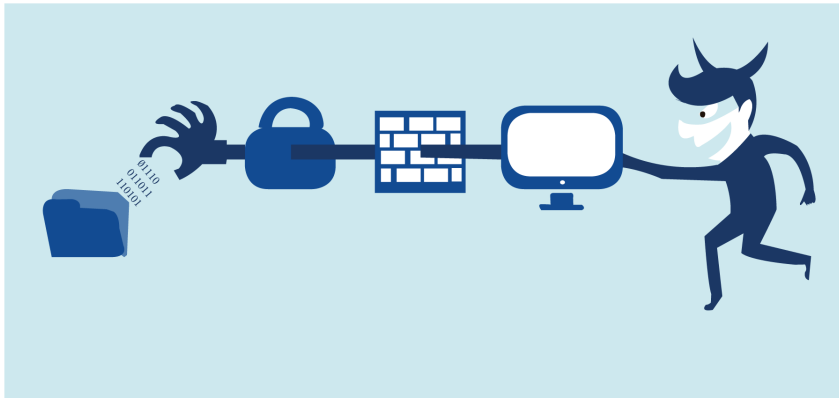
Figure 1: Cybersecurity Maturity Model

The Threats

On March 2016, the server of the Philippine Voters' Database was reportedly hacked by Anonymous Philippines in which at least 54 million sensitive data⁸ was leaked into the Internet, including 1.3 million passport numbers of Filipinos working overseas. According to common news articles reported by various newspapers, the breach into the system occurred through the use of SQL injection. The alleged hacker was arrested by the National Bureau of Investigation after the IP address was discovered and tracked down.

In 2016, at least 68 government websites have been subjected⁹ to attacks including attempts

8 <http://cnpilippines.com/news/2016/06/17/Comelec-hack-data-breach.html>



Most of the organized cybercriminal groups operating in the South East Asia Pacific region are hosted by the criminal market place services in Central Asia, South East Asia, as well as West Africa. It is also difficult for the Philippines and international law enforcement agencies to prosecute them when there is limited jurisdiction or no extradition agreements.

Malware that are developed and deployed are increasingly advancing and their impacts are not fully documented in the Philippines as we have yet to establish a National Database for computer incidences. The increasing use of ransomware and threats of distributed denial of service (DDoS) are just examples of how these cybercriminals are becoming increasingly aggressive and confrontational.

Hacktivist

Hacktivist groups are motivated by issue and mostly function in decentralized fashion. Some schools of thought are espousing the idea that web defacement and replacing them with political messages is an exercise of their freedom of speech. They select their targets based on their perceived grievances. There is a vigilante quality to their acts, as demonstrated by the hackers who attacked a certain government website. Their methods of attacks are mostly defacement and distributed denial of service (DDoS). However, some hacktivists are able to inflict greater and often lasting damage to some of their victims.

Script kiddies

Attention has not been fully given to these so-called script-kiddies, but they are threats nonetheless. They are generally less skilled individuals. However, if they know how to access the black market, there are services and even hacking guides available and can be accessed through the Internet. However, these script kiddies have not been fully assessed in terms of the damage and impact they can effect towards their target organizations.

Terrorists

Terrorists operate with specific intent and motive and that is to create chaos and terror to the public. Some terrorists use the Internet as an effective recruitment tool for vulnerable target groups or individuals. Although their technical capabilities are generally low, the low sophistication of their disruptive activity (defacement or DDoS) will have an impact even in moderate scale. Furthermore, as they exploit the Internet to recruit talents and even exchange technical skills, the opportunity of being able to enlist an established insider is likely to increase as well.

Non-State and State-sponsored threats

Countries with technical capabilities to attack other states are increasing. The first world countries are most prone to frequent attacks. However, other countries like the Philippines may be used as launch pads to attack other states either by another state or through state-sponsored attacks. Developed nations continuously improve their capabilities to deflect, defend and deter these attacks at a steady pace. But by the same token, states with technical capability to attack these

developed nations, often use basic tools and techniques against vulnerable targets frequently exploiting discovered gaps between the systems of these states because of poor defenses. These attacks are no longer confined within espionage but there are hostile threat actors that have developed and deployed cyberattacks with destructive objectives. Therefore, all states are at risk and can have their national security threatened from potential attacks through the CII and overriding the industrial control systems. Thus, the Philippine Government through DICT shall mandate that CII protection and security are prioritized by CII owners following the minimum guidelines that shall be set by the National Government based on the plan.

Insiders

Insiders and trusted employees are at the top of the food chain that is frequently exploited by criminal groups, terrorists, hacktivists, or non-state and state-sponsored attackers through social engineering, clicking on phishing email, plugging infected USB into a computer, or ignoring security procedures of the organization. Although some may be unintentional actions, their privileged access to the systems and data can create as much adverse impact and damage to the organization.

9 <http://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked>

10 <http://cnnphilippines.com/news/2016/08/05/South-China-Sea-RAT-cyber-attack-Philippines.html>

THE NATIONAL STRATEGIC CONTEXT



THE NATIONAL CYBERSECURITY PLAN 2022

SECTION 4

This section covers the general details of the strategy, including the implementation plan for NCSP, since this document shall be the blueprint for the protection of the CII of the government, public and private networks. The strategy is still a work in progress and will be reviewed for improvement on a regular interval concurrent with its implementation. It will follow the PDCA Cycle (Plan → Do → Check → Act).

However, the priority program areas will be the starting point in establishing and working towards the goal of reaching a mature cybersecurity state. Results in the implementation of the plan shall be monitored closely and regularly. Data shall be collected from stakeholders and shall be collated into a national database for incidences on cyberattacks, intrusion attempts or disruption of systems, and other sources of threats whether intentional or accidental.

Initial metrics that have been prepared and proposed within this strategy shall be agreed upon by the stakeholders to create ownership and involvement among everyone. The following sections describe the general areas that will be prioritized.

THE NCSP 2022 VISION

The National CyberSecurity Plan 2022 shares its vision to reach the state of having a “Trusted and Resilient Infostructure.” In order to accomplish this state, the following mission objectives have been determined:

- a. To systematically and methodically harden the Critical Information Infrastructure (CII) for resiliency;
- b. To prepare and secure government Infostructure;
- c. To raise awareness in the business sector on cyber risk and use of security measures among businesses to prevent and protect, respond and recover from attacks; and
- d. To raise awareness of individuals on cyber risks among users as they are the weakest links, they need to adopt the right norms in Cybersecurity.

Metrics shall be developed to monitor the implementation progress of the plan based from the above objectives. There are three guide questions that will aid in jumpstarting the cybersecurity strategy of government agencies. The strategy can be replicated and adopted by agencies as it is rolled out and cascaded to the smallest unit of the government.

- i. Where are we now? (Conduct of inventory of information assets, information systems, computer systems, network systems, and security systems)
- ii. What do we want to achieve? (Setting, aligning, and harmonizing cybersecurity targets of each agency with NCSP)
- iii. How do we get there? (Establishing the roadmap)

STRATEGIC INITIATIVES

The strategic initiatives of the government focus on the technical, administrative and procedural measures. The strategy shall cover strategic programs for:

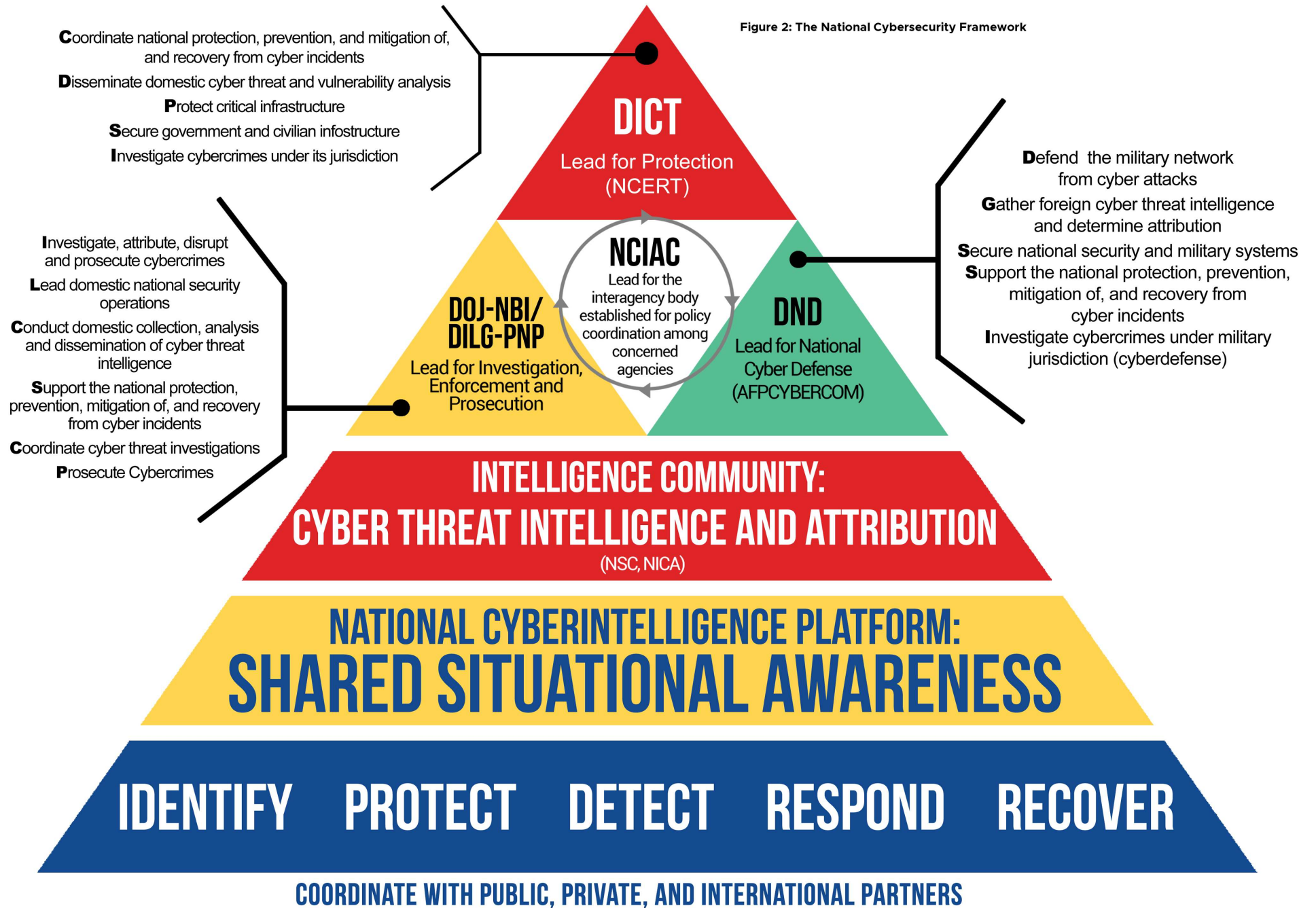
- a. Enhancing security resilience of the CII and government, public, and military networks to deal with sophisticated attacks;
- b. Increasing efforts to promote adoption of cybersecurity measures among individuals and businesses; and
- c. Growing pool of cybersecurity experts.

THE NATIONAL CYBERSECURITY FRAMEWORK

In the development of the National Cybersecurity Framework, one has to understand the interrelationship¹¹ between cybersecurity and cybercrime. Cybersecurity and cybercrime can be distinguished in the context of the law. Cybersecurity relates to the confidentiality, integrity, and availability of computer systems, network systems, information systems, and other areas related to the protection of information assets. Therefore, the framework focuses on technical, administrative, and procedural measures that will protect critical infrastructure and increase resilience of ICT and ICT-enabled environments. Cybercrime relates to the penal law that punishes crimes¹² committed with the use of computer systems or in some cases, attacks by the criminals on the system itself. It pertains to the crimes that affect the confidentiality, integrity, and availability of data and computer systems.

¹¹ Department of Justice – Office of Cybercrime. National Cybercrime Strategy 2016-2022. pp. 3

¹² Section 4 (a) of Republic Act No. 10175. (2012).



The thrust of the cybersecurity framework is to build the trust and confidence on ICT and cyberspace. Cybercrime on the other hand, has its strategy anchored on crime prevention and criminal justice to ensure that the rule of law applies in ICT and cyberspace. In other words, cybercrime focuses on investigation and prosecution (reactive state) while cybersecurity is on security and protection (proactive state).

Figure 2 illustrates how the concept was developed. The Framework is composed of three layers where all three key players are interrelated but have distinct functions. Their sets of activities are planned and programmed according to their mandates. However, these activities shall work in synergy with its counterparts through a cooperative, collaborative, and coordinated environment.

The driver for the framework is the strategy under NCSP. The apex of the pyramid also illustrates the interrelationship between all key players and its corresponding roles to implement the NCSP. Emphasis is given also on the importance of collaborating with public, private, and international partners.

The next layer indicates that sharing of intelligence such as data and information is crucial to identifying potential threats, simulating scenarios, studying threats and incidences, or developing innovative measures through continuous monitoring and evaluation of information shared by stakeholders in a timely manner.

The middle layer shall establish an environment for sharing situational awareness. The concept of sharing of information acts as an enabler for integrated operational actions which can be orchestrated simultaneously or in parallel with one another is invaluable to the entire lifecycle of incident response management.

The bottom layer is where responses to incidences and events are recorded, monitored, evaluated, and analyzed which will provide input to improvements on processes, policies, guidelines, or procedures. As stated earlier, the country's cybersecurity capabilities are still at its infancy stage, therefore, the core framework in the protection of the CII shall adopt the NIST Cybersecurity Framework¹³ as a starting point with the following core functions: Identify → Protect → Detect → Respond → Recover. The activities under these functions can be conducted concurrently and continuously.

In developing the policy to implement the strategy using the framework, the government through DICT shall adopt the proactive approach instead of being reactive. We have to think and strategize a couple of steps ahead of the cybercriminals. The government must take necessary measures to be adaptable to the future social changes and potential risks through constant and continuous analysis of information and data that have been gathered.

THE GUIDING PRINCIPLES

Framing of the vision, its objectives and creating the framework is guided with the principles on the following:

The Rule of Law

Cyberspace is a vast place with many new and emerging areas still relatively unknown and unexplored. However, the rule of law is as much applied to the cyberspace as it is strongly and strictly observed in the physical world to ensure that there is order in our society.

Autonomy and Self-Governance

Cyberspace thrives in autonomous systems that are run, managed, and operated by various owners. The Government intends to continue respecting the self-governance that cyberspace has developed. The foundation of cyber governance is the ability of every individual or group to be self-reliant and responsible users of the Internet. Every individual or group observes the established universal values and norms such as freedom, democracy, peace, and stability within cyberspace, as it is used by diverse individuals or groups from all over the world.

Collaboration with Multi-Stakeholders and International Cooperation

Collaborating with multi-stakeholders and establishing international cooperation enables a community of practice where information is shared among these key stakeholders. Layers of defense can be built through the cooperation of the citizens, the businesses and organization, the education providers, governments, and the whole



society in general. Protection and prevention from multi-dimension groups will minimize and manage these cyberattacks to minimum adverse impact.

Balance between Free Flow of Information and Privacy Rights of Individuals

The rights of every individual to have equal access to the Internet are upheld at all times. However, balance must be made between protecting the privacy of the individual against securing protection of information and data of the users.

Risk Based Management Approach

is another guiding principle of the strategy. One of its national targets is the protection and security of the CIIs. This approach provides a comprehensive preparation in the formulation of a Risk Treatment Plan that the government and other relevant sectors will eventually undertake as it evaluates and thoroughly considers the type of risk appetite of the stakeholders.

¹³ National Institute of Standards and Technology.(2014).Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

ROLES AND RESPONSIBILITIES

The roles and responsibilities of the stakeholders and key players must be defined so that the functions of each stakeholder will be in synergy with the activities of other stakeholders. The strategy provides clarity in the relationship and interrelationship among the stakeholders.

The job of making sure that cyberspace is safe and secure is a collective effort that is shared by each and every one of us. The government is just a single piece in the macrocosm of cyberspace.



Individuals

Individuals have a large role to play since it is the biggest population base in the internet. In the same manner that we put value of securing our personal assets in the physical world, the same consciousness of practice must be observed in cyberspace. The cyber environment is vast and the capacity of the government to patrol the cyber community is limited. However, the individuals who created the cyber community may act as a force multiplier and provide a neighborhood watch against malicious individuals prowling the Internet.



Business and Organizations

The heads of industry organizations are drivers of our economy. Institutions such as banking systems composed of our financial institutions, together with the business sector, create one of the pillars of our country's economy.

Government

Table 1 provides a brief description of the governments functions and mandates and the interrelationship of processes as well as interdependencies of the key players in keeping our information systems, computer systems, and network systems accessible, available, and functioning at all times and free from any interruptions or disruptions, whether intended or unintended.



NATIONAL AGENCY

DICT

- Ensure the rights of individuals to privacy and confidentiality of their personal information
- Ensure the security of critical ICT infrastructure
- Ensure the security of information assets of the governments, individuals, and businesses,
- Provide oversight over agencies governing and regulating ICT sector
- Ensure consumer protection and welfare, data privacy, and security
- Formulate a national cybersecurity plan
- Formulate, recommend, and implement national policies, plans, programs, and activities related to cybersecurity activities
- Assist and provide technical expertise to government agencies in the development of guidelines in enforcement and administration of laws, standards, rules, and regulations governing cybersecurity
- Assess the vulnerabilities of cybersecurity
- Issue updated security protocols to all government employees in the storage, handling, and distribution of all forms (e.g. digital, electronic, snail mail, etc.) of documents and communications. Enhance public-private partnership for information sharing involving cyberattacks, threats, and vulnerabilities to cyber threats
- Conduct periodic strategic planning and workshop activities to reduce the country's vulnerabilities to cyber threats
- Establish linkages for coordination on domestic, international and transnational efforts related to cybersecurity

CICC

- Extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT)
- Coordinate the preparation of appropriate and effective measures to prevent and suppress cyber crime activities
- Monitor cybercrime cases being handled by participating law enforcement and prosecution agencies
- Facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression, and prosecution
- Coordinate the support and participation of business sector, local government units, and non-government organizations in cybercrime prevention programs and other related projects
- Recommend enactment of appropriate laws, measures, and policies
- Call upon any government agencies to render assistance in the accomplishment of CICC's tasks and functions
- Perform other matters related to cybercrime prevention and suppression, including capacity building and other functions and duties necessary to implement its mandated functions

Table 1.a - Roles and Responsibilities of Key Stakeholders

LAW ENFORCEMENT AND PROSECUTION AGENCIES

- Investigate, attribute, disrupt, and prosecute cybercrime
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation, and recovery from cyber incidents
- Coordinate cyber threat investigations
- Prosecute cybercrimes

NATIONAL DEFENSE (MILITARY)

- Defend the country from cyberattacks
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cybercrimes under military jurisdiction (cyberdefense)

Table 1.b - Roles and Responsibilities of Key Stakeholders

The government through DICT shall provide the formulation of policies, guidelines and strategic direction for cybersecurity. The CICC, being a coordinating center for CERTs and LEAs, as well as international linkages, shall promote cooperative, coordinated, and collaborative environment for all stakeholders. The NCERT is the operating arm for implementing programs, projects, and activities for computer emergency responses.

Although Table 1 has already described in general the roles and the responsibilities of the major key stakeholders, the governance and management structure shall be fleshed out during stakeholders' consultation to bring a cohesive and coherent governance structure and eliminate duplication or dysfunctions in the course of implementing the Plan.

Roles and Responsibilities of Heads of Agencies

It is also noteworthy to mention that the heads of agencies are the first line of defense in the protection of the CII. The following functions shall also be mandatory to their existing functions and the functions of their agencies:

- Assess the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support operations or assets under their control;
- Determine the levels of information security appropriate to protect such information and information systems;
- Implement policies and procedures to cost-effectively reduce risks to an acceptable level; and
- Conduct periodic testing and evaluation

of information security controls and techniques to ensure that they are effectively implemented.

KEY AREAS FOR CYBERSECURITY

There are several layers in security that the strategy shall focus on and shall prioritize for the development and implementation of its policies, plans, programs, and guidelines for security and protection. To put emphasis, cybersecurity relates to actions that stakeholders must take to establish and maintain security in cyberspace. The other domains of security¹⁴ are necessary in implementing the protection of CII.

Information Security

Information security talks about confidentiality, integrity, availability, authenticity, and nonrepudiation, of information as an asset of the organization. We look at the strategy from a multi-dimensional perspective. As mentioned earlier, the digitization of the world has made everything interconnected and interdependent, from man to machine through ICT enabled-technology, internet, mobile-based devices, or smart devices (the concept of Internet of Things or IoT). This is achieved through the application of policy, education, training and awareness, and technology. The government aims to institutionalize information security across all government agencies down to the smallest operating units of the government. The NCSP shall provide the guidelines and the minimum compliance requirements to jumpstart implementation of information security in the government.

¹⁴ International Organization for Standardization. (2012). Information Technology – Security Techniques – Guidelines for Cybersecurity, 1st Edition (ISO/IEC 27032:2012). Published in Switzerland



Application Security

Application security is a process performed to apply control and measurements to application systems to manage deployment and use risks. These controls and measurements are applied to the application itself (e.g. processes, components, software, and results), to the data (e.g. configuration data, user data, organization data), and to all technology, processes and stakeholders involved in the application's life cycle.

When we develop the applications, security should be embedded and stressed into every stage of the System Life Cycle Development (SLDC). Security assessment of applications is conducted after it is developed and these issues are fixed. There are malicious actors whose only intention is to break into the computer systems and network systems to damage them, whether for fun or for profit.

Conducting application testing on a regular basis will mitigate and identify system vulnerabilities. Currently, vulnerability assessments for applications developed are not fully implemented and institutionalized across all government agencies, especially those that operate critical systems.

Network Security

Network security covers design, implementation, and operation of networks to achieve the purpose of information security on networks within the government and public network, between these networks, and between government and public network and the users.

Intrusion detection methods and traffic analysis are one of the most basic security measures we can implement to ensure the security of our systems. Auditing and

monitoring our networks and perimeter systems require a thorough understanding of our network architecture and how attackers can exploit gaps in between these network systems. Technological advancement and the growing number of available of network hacking tools have increased the threats into our systems. As a way to combat the growing problem, inventory of devices that are connected into our network is recommended. The strategy includes the inventory of the government and public network.

Internet Security

The objective of internet security is to protect internet-related services and ICT systems and networks as an extension of network security in organizations including in the privacy of homes. It also ensures the reliability and availability of internet services.

Everyone uses the internet. The risks that the internet poses such as data and information that flows across the cyberspace through a series of computers and network links are highly likely to happen. Various threats over the internet must be fully understood. One of the vulnerable groups with high exposure in the internet is small business-owners, especially since the use of the e-commerce platform has gained momentum. Raising the awareness will help reduce the risks and the vulnerabilities.

15 Harp, D. , Gregory-Brown, B. IT/OT Convergence, NEXDEFENCE.=, <https://docs.google.com/document/d/1Lj9MeZbA2u63AVlbseVOWRmrnA8BaNfjKNzq4m nksQ/edit?ts=58af77d6>

CII Protection

Systems and networks that are operated by critical infrastructure providers (e.g. telecommunications, water resource agencies, or power generators and plants) must be protected and secured.

The critical information infrastructure also known as the critical infrastructure (CII) plays a vital role in our economy. Adopting the approach of Integrating Information Technology with Operational Technology in protecting critical infrastructure is essential to the objectives. When Operational Technology¹⁵ (consist of hardware and software systems to monitor and control industrial controls including building control systems, air/land/sea transportation control systems, etc.) is deployed together with Information Technology¹⁶ (refers to application of computers to transmit, processes and store data the security defense in depth becomes robust. The purpose of converging these two methods will ensure protection of both the front and back ends from intrusion and potential attacks.

In 2001, the Government indicated that the list¹⁷ of "critical infrastructure includes, without limitation, power plants, power transmissions and distribution facilities, oil and gas depots, key public work structures, vital communications installations, public and

16 Harp, D. , Gregory-Brown, B. IT/OT Convergence, NEXDEFENCE.=, <https://docs.google.com/document/d/1Lj9MeZbA2u63AVlbseVOWRmrnA8BaNfjKNzq4m nksQ/edit?ts=58af77d6>

17 Sec. 10, Memorandum Circular No. 37, s. 2001, Providing Four Pillars of Policy and Action of the Government Against Terrorism.

private buildings and other facilities in the center of commerce and industry”. The NCSP 2022 expanded this list and adopted the CII list from the Cybersecurity Strategy of Singapore . The list includes, but not limited to, government and emergency services, business process outsourcing, healthcare, media, banking, financial, power, water, telecommunications, transport and logistics. This was also classified according to Services, Utilities, and Transport that cuts across all sectors. Our CII must have the resiliency to operate against information security risk, network security risk, Internet security risk, and cybersecurity risk.

Furthermore, government’s commitment to protect itself and public CII starts with adopting clear policy objectives at the highest level of government. The strategy shall include the steps to enhance the security level components of information system and networks that constitute CII. Risk assessment shall be conducted based on the analysis of vulnerabilities and threats to the CII. A periodic review on the national risk management process will help implement the risk management strategy at every level.

It is however emphasized, that the owners of CIs will have the primary responsibility to secure and protect these systems. The government can only do so much having very limited resources such as manpower and financial resources. But together with other system and CII owners, we will be able to create multi-layers of security and defend our cyberspace and protect our CII.

18 Singapore’s Critical Infrastructure Sectors, Singapore’s Cybersecurity Strategy, pp. 11

CLASSIFICATION OF NATIONAL SECURITY SYSTEM

The term national security system means, “any information¹⁹ system (including telecommunication system) used or operated by any agency or outsourced to a third party by an agency”:

The function, operation, or use of which:

The function, operation or use of which:

- i. Involves intelligence activities;
- ii. Involves cryptologic activities related to national security;
- iii. Involves command and control of military forces;
- iv. Involves equipment that is integral part of a weapon or weapons system; or
- v. Critical to the direct fulfillment of military or intelligence missions.

Protected at all times by procedures established for information that have been specifically authorized under criteria in an Executive Order or an Act of Congress to be kept classified in the interest of national security or foreign policy.

Exclusions from National Security System Clarification

There is also the need to have a distinction between a National Security System (NSS) and those that are not covered by the parameters for classifying the NSS. The systems that are not included are systems

19 National Institute of Standards and Technology. (2003). Information Security: Guideline for Identifying an Information System as a National Security System (NIST-SP 800-59). U.S. Department of Commerce. Barker, W.C.

that are used for routine administrative and business applications (including but not limited to payroll, finance, logistics, and personnel management applications).

RISK MANAGEMENT APPROACH

The methodologies for CII protection is through the Risk Management Approach. The government shall manage its risks in the protection of the CII by identifying, analyzing, and evaluating risks. The management of the risk must be integrated into the overall governance, strategy, planning, implementation, management, reporting processes, policies, values and culture²⁰.

Guidelines for implementing the risk management approach shall be formulated by the government through

DICT. Under the guidelines, critical systems and CII owners shall formulate their risk management policy based on its mission critical objectives, business processes and operational environment needs.

Risk Assessment

To implement the risk-based management approach, the government must conduct the three stages of risk assessment: identification, analysis, and evaluation. In the formulation of the risk evaluation criteria, the primary and mandatory consideration shall be on the NSS and CII. The risk management policy that government agencies shall develop appropriate to their agency’s mandate and mission, must be aligned with NCSP vision and mission objectives.



20 International Organization for Standardization. (2012). Risk Management – Principles and Guidelines (ISO/IEC 31000:2009). Published in Switzerland.

STRATEGIC COLLABORATION



Establish National Level Committee

National Cybersecurity Inter-Agency Committee (NCIAC)

The National Cybersecurity Inter-Agency Committee (NCIAC) was created in 2015 through Executive Order No. 189. This initiative of creating a single coordinating NCIAC is geared towards a more efficient and effective strategic planning and implementation of measures with an ultimate goal of strengthening cybersecurity capabilities against existing and future cyber threats and all other challenges with respect to cyberspace. The National CIAC would serve as a centralized hub to harmonize and integrate national efforts relating to cybersecurity.

Cybercrime Investigation and Coordination Center (CICC)

The Cybercrime Investigation and Coordination Center was created through the Cybercrime Prevention Act of 2012 (R.A. 10175) function as a coordinating body. The CICC also facilitates collaboration, cooperation, support, and participation from multistakeholders and the international bodies for cybersecurity related activities.

Public Private Partnership

Public Private Partnership Forums

The government cannot take on the challenges and threats from cyberspace by itself. However, creating environments such as forums for sharing and exchanging information will provide an avenue for a public-private partnership. The first step to a partnership is to have a good communication relationship with its stakeholders.

International Collaboration

The strategy shall not only focus its efforts on local and domestic collaboration with its partner and counterpart agencies for cybersecurity related matters, but shall also forge international collaboration.

As the government prepares the environment for coordination, partnership, and collaboration across all levels and sectors of the government and society, the concept shall also encourage the creation of a Community of Practice. Thereby upholding one of its guiding principles, collaboration with multi-stakeholders shall also help build the cornerstones of a resilient ICT-enabled governance.

KEY STRATEGIC INITIATIVES



The implementation of the NCSP, as indicated previously, hinges on the national priority targets and the underpinning principles that will also guide the formulation and preparation of its implementation plan. Thus, there are five strategic initiatives that shall be orchestrated under the DICT.

KEY PROGRAM AREAS

PROTECTION OF CII



As our government works towards digital governance, the support infrastructures that power our virtual environment must be able to sustain operation before, during, or after any cyber incidences or attacks. To fully understand the importance of the critical information infrastructure in the digitization of our government, we look at how this was described²¹: information components supporting the critical infrastructure, and/or; information infrastructure supporting essential components of government business, and/or; information infrastructure essential to the national economy.



For the purpose of this document, we shall define critical information infrastructure as, “critical infostruture whose failure or limited operation due to natural or man-made disasters would surely cause a tremendous impact on the majority of citizens.”



However in order to bring everyone on the same page, this document will adopt the elements of infostructure, whether physical or virtual, cited under the Cybercrime Prevention Act of 2012²² as follows: computer systems, and/or networks, and/or computer programs, computer data and/or traffic data.



Furthermore, it is also emphasized that such infostructure is so vital that interference and/or destruction of such systems and assets will have debilitating impact on national security, economic security, national public health, public safety and order.

To determine and establish the resiliency of our CIIs, the government will focus on two major activities that will help establish the baseline for our cybersecurity capability and capacity in the protection of our critical infostructure: Compliance and Assessment and 2) National Drill Exercises.

The compliance and assessment shall be composed of three levels:1) Protection Assessment (inventory level), 2) Security Assessment (readiness) and, 3) Compliance to Cyber Risks to CII (voluntary).

Cybersecurity Assessment and Compliance

- i. Protection Assessment Project (ICT Systems)
- ii. Security Assessment Project (Readiness)
- iii. Certificate of Compliance to Cyber Risks to CII(Voluntary Program)

The strategic initiative of protecting the CII under levels 1 and 2 shall become a standard practice and will work as complementary to the preparation of the Information Systems Strategic Plan (ISSP) of any government agency. Since the ISSP is the blueprint of the digital environment of a government agency, this is an appropriate vehicle to ensure that compliance and assessment are institutionalized during implementation and

becomes embedded into the regular programming of a government unit. Level 3 on the other hand is a voluntary program where government agencies may be assessed by a third party institution (Certifying Body or other institutions that promote compliance to standards). This program, although still proposed as a voluntary program, in turn will institutionalize the goal of implementing a resilient ICT environment for the government.

However, agencies and organizations classified as CII shall have mandatory compliance to Level 3 and government agencies and organizations with sytems that have been classified under National Security System shall be compliant with the requirements relevant to standards on Information Security (ISO/IEC 27000).

Establish Program for National Cyber Drills and Exercises

After establishing the baseline results for assessment and compliance, government units shall participate in National Cyber Drills and Exercises. This shall become a mandatory compliance for all government agencies in order to sustain the development of our cybersecurity towards the desired maturity level of our systems.

Figure 3 illustrates the cybersecurity maturity model²³ and the agility state we desire to achieve the Resilient Enterprise. We will not be able to defend well if we do not know our strengths and weaknesses. Therefore, in conducting a self-assessment, the level of the agility and speed of response

during cyber-attacks must be determined.

At Reactive and Manual state, a doctrine and the primary concern is to put out fires as opposed to finding the cause of the fire and preventing the fire from spreading.

At the Tools-Based state, tools and technologies are used to assist people in reacting faster.

At the Integrated Picture state, the focus is on interoperability where standards are based on data exchange for situational awareness.

At the Dynamic Defense state, operation functions are on a predictive and agile level because the events are reviewed and analyzed to help the responders and operators identify, detect, mitigate, and recover from these attacks.

At the Resilient Enterprise state, the objective is predictive and mission-focused to isolate and contain damage, secure supply chains, and protect key critical infrastructure to continue operation through cyber-attacks.



21 Mansfield, N. Organization for Economic Co-Operation and Development. Development of Policies for Protection of Critical Information Infrastructure. 2007. South Korea.

22 R.A. No. 10175, Sec. 3 (j).

23 Lentz, R.(2011).[PowerPoint slides]. <http://www.dintel.org/Documentos/2011/Foros/ses2Mcafee/lentz.pdf>

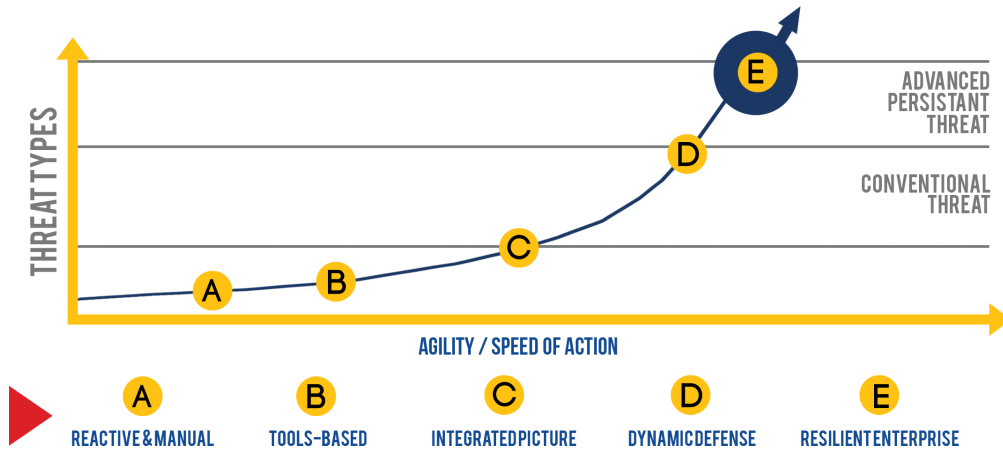


Figure 3: Cybersecurity Maturity Model

The cybersecurity maturity level of the country is still mostly at a Reactive and Manual state. The goal of NCSP is to reach the state of developed resiliency and the ability to sustain operations during and after cyber-attacks. The NCSP is the roadmap that will enable the government to reach the Resilient Enterprise state.

Establish National Database for Monitoring and Reporting

Currently, the country has no single authority that manages a national database and monitors threat reports, including intrusion attempts and other computer incidences. The data and information remain in silo with different agencies. To effectively identify and protect our CII against potential threat attacks, complete information source and availability of data must be accessible at all

times to authorized government agencies and personnel. The data and information that are collected can be used for research and development, policy updates and formulation, threat analysis, analysis of emerging trends and patterns, etc.

Reporting²⁴ of security breaches and intrusion attempts including other computer incidences or events shall be mandatory to all government agencies including agencies and offices that have centralized collection and repository of information. The data and information that have been collected shall become a valuable component for developing and preparing innovative measures in protecting and defending our cyberspace.

PROTECTION OF GOVERNMENT NETWORKS

The government in its national security policy²⁵ has recognized the growing dependence of government, transportation, industries, and economy on all components of cyberspace. The growing dependence increases the level of exposure and vulnerability to cyberattacks. These are cyberattacks that could lead to the paralysis of communication infrastructure, international financial systems, critical government services and defense/military command and control systems.

Establishment of a National Computer Emergency Response Program

A program for the national computer emergency shall be established and guidelines shall be formulated to aid government agencies in the event of a cyberattack or cyber incidents, including prolonged cyberattacks. A well-prepared emergency response protocol should become part of the operational environment of any government agency down to the local government unit. The program shall include the development and formulation of the Computer Emergency Strategic Communications Plan. This shall form part of the National Drill Exercise which shall be done on a periodic interval.

Establishment of CISO Programs in Government Agencies

To implement the strategy efficiently, it is recommended that CISO Programs are

established into Government Agencies and the Local Government Units. CISOs have an important role to play in security governance. The general responsibilities²⁶ of a CISO includes but not limited to:

- i. Integrating information security measurement into the process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;
- ii. Obtaining the adequate financial and human resources to support information security measurement program development and implementation
- iii. Leading the development of any internal guidelines or policy related to information security measures;
- iv. Using information security measures in support of the agency's CIO's annual report to the agency head on the effectiveness of the agency's information security program, including progress of remedial actions;
- v. Conducting information security measures development and implementation;
- vi. Ensuring that a standard process is used throughout the agency for information security measures development, creation, analysis, and reporting; and
- vii. Using information security measures for policy, resource allocation, and budget decisions.

24 Data Privacy Act of 2012, R.A No. 10173 Section 20 (c)(4) and (f).(2012)

25 National Security Council.(2011).National Security Policy 2011-2016: Securing the Gains of Democracy, pp.20. <http://www.gov.ph/downloads/2011/08aug/NATIONAL-SECURITY-POLICY-2011-2016.pdf>

26 National Institute of Standards and Technology. (2008). Information Security: Performance Measurement Guide for Information Security (NIST-SP 800-55 Revision 1). U.S. Department of Commerce. Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. & Robinson, W.



The strategy requires that agencies provide appropriate protection of their resources through implementing a comprehensive information program. The program that each agency implements should be commensurate to the sensitivity of the information being processed, transmitted, and stored within the information systems of the agency.

The CISO Program shall be jumpstarted with a series of training and capacity building activities to fully equip personnel who shall be given the assignment to function as a CISO in an agency.

Establishment of the Computer Emergency Response Structure

The Computer Emergency Response Program shall be composed of the National CERT, Government CERTs and the Sectoral CERTs. The National CERT is the highest body for cybersecurity related activities. All CERTs, Government CERTs, Sectoral (or Private) CERTs, as well as organizational CERTs shall coordinate and report incidences to the National CERT. Figure 4 illustrates the hierarchy of the Computer Emergency Response structure in the country.

However, the CERTs all over the country shall also conduct real-time coordination²⁷

with CICC as provisioned in the law.

- i. National Computer Emergency Response Team (NCERT)
- ii. Government Computer Emergency Response Team (GCERT)
- iii. Sectoral Computer Emergency Response Team (Sectoral and Private CERT)
- iv. Organizational Computer Emergency Response Team (Organization Level CERT)

Apart from establishing the hierarchy of CERT in the country, governance structure shall be clearly defined to make the implementation of the NCSP efficient and the monitoring of its progress and milestones more effective to ensure that the plan shall be on target with its objectives until 2022.

Basic Computer Emergency Response Program

The strategy will include projects that will provide basic computer emergency response awareness to government IT employees. IT personnel, although they have technical understanding, may not be fully aware of how to respond to a computer security incident that may compromise the system.

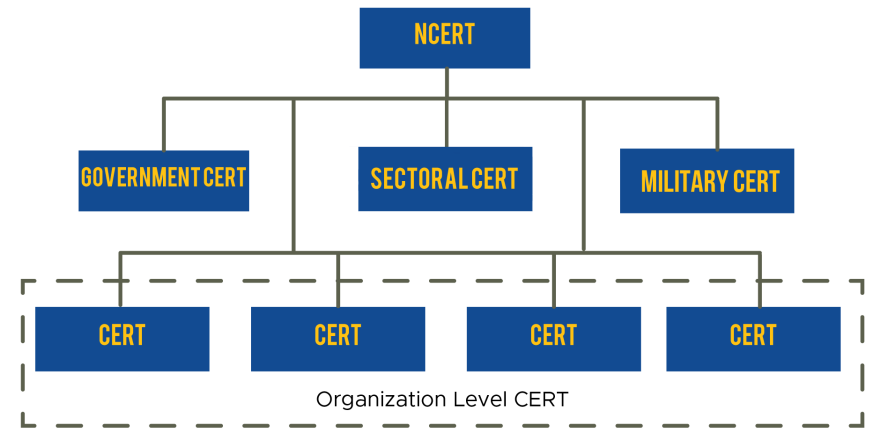


Figure 4: Hierarchy of Computer Emergency Response in the Country

Building the capability of the CERT of government agencies will take time to be developed and considerable investment for training will have to be planned accordingly. Therefore, the first step is to build the awareness and leveling of the understanding of how computer emergency response works, what to do in the event of the attack, who to report to, and how to deal with the impact of the cyber-attacks. This will serve as preparatory stage while the agencies are still in the organizing stage (CERT building). The government will provide training programs, such as Training of Trainers, Basic Computer Emergency Response, etc.

The program shall include regular communication drill exercises to synchronize the communication practices and protocols of all CERTs during cyber-attacks. All CERTs must assign focal personnel to attend meetings and coordination that shall be established and scheduled at regular intervals. The objective of the government is to ensure that communications and coordination with CERTs all over the country are firmly established as we try to prepare and ensure that we work together towards a resilient ICT

environment through CII protection of government and public networks.

Capacity Building and Capability Development Program

Cultivating existing talents and developing new ones are long term development plans and the investment shall be substantial. The government needs to acquire and strengthen its capabilities to protect against any cyber threat. This means we need to develop and retain talented and qualified cybersecurity professionals. The government shall engage and collaborate with the academe and other educational institutions to support the development of cybersecurity specialists through curriculum development. Much like the need for skilled workforce to support the Outsourcing Industry, the gap between demand and supply for key cybersecurity roles must be addressed now. The lifeblood of any organization is to have a skilled workforce. The lifeblood to secure our cyberspace is to have skilled cybersecurity specialists.

27 Cybercrime Prevention Act 2012. R.A No. 10175 Section 26 (a). 2012

Establish Pool of Information Security and Cybersecurity Experts

The government shall maintain a list of Information Security and Cybersecurity Experts. This can be accomplished through several activities:

- i. Establish Cyber Training Facilities and Certification Programs
- ii. Promote National Cybersecurity Research and Development Program to attract and cultivate cyber experts
- iii. Establish Training Programs to Develop Cybersecurity Specialist
- iv. Promote Communities of Practice (COP)

Establish Threat Intelligence and Analysis Operations Center

One of the long term programs of the strategy is to establish a Threat Intelligence and Analysis Operations Center. The concept is mainly to provide a facility to house Research and Development, Testing Laboratories and Live Test of Threats and Threat Scenario Simulators. The National Database provides a repository of information from all over the country to gather data and intelligence that are analyzed on a regular basis by technically competent Analysts. Data collection and intelligence gathering are two basic methods for developing and building up our defense in depth. Building the competence of our threat intelligence and analyst through studying the various cyber incidences and cyber-attacks will improve our capability and capacity against future cyberattacks. The government through CICC and NCERT shall coordinate and collaborate with other government agencies with existing facilities that function as threat intelligence and analysis operations center.

- i. DND Cyber Defense Center
- ii. NSC Threat Operations Center
- iii. AFP Cyber Command
- iv. NICA Cyber Intelligence and Attribution Center

Protection of Electronic Government Transactions

There are enabling laws such as the Electronic Commerce Act of 2000²⁸ which provides the basis²⁹ for employing cryptography as a means to protect the integrity and authenticity of the documents that are processed during government transactions. The Plan shall provide recommendations on policies that will have impact on the digitization of government transaction and formulate guidelines that will include the protection of the electronic document in transit, at rest, or during processing using cryptography tools.

Update of Licensed Software

Software patches, and software (including hardware devices such as servers, network devices, etc.) approaching its end of life cycle support are also potential sources of threats. The NCSP strategy requires that all departments, bureaus, offices, and other agencies of the national government including constitutional commissions, congress, the judiciary, state universities and colleges, government owned or controlled corporation, and the local government units, shall exercise mandatory review of all its existing software licenses, machines and devices to ensure that all necessary components are up to date and are still well within its life cycle period.

For protection of Military Networks, there will be a Military Computer Emergency Program. Under which is the DND Defense Situation Monitoring Center for Policy and the AFP Cyber Command for Operations.

For intelligence, a Threat Analysis Center will be established under the NSC. The operating arm will be the NICA Cyber Intelligence and Attribution Center.

²⁸ Electronic Commerce Act of 2000. R.A. 8792. 2000.

PROTECTION OF SUPPLY CHAIN

National Common Criteria Evaluation and Certification Program

- i. ICT Equipment Security Evaluation and Certification Project
- ii. Benchmarking Project

The challenges in cybersecurity are multi-dimensional. Therefore, the need to approach it from a multi-disciplinary perspective is important. The objectives of Supply Chain Protection are to promote secure and efficient movement of goods and foster a supply chain system that is prepared for and can withstand evolving threats and hazards, and the ability to rapidly recover from disruptions. In order to achieve this, the strategy will work on enhancing the risk management efforts that will include addressing unknown risks to managing the risk in the supply chain.

Apart from the strategy of employing the risk management approach, the government will also employ the common criteria to determine compliance of the supplier, as well as establishing the guidelines to conduct benchmarking to ensure that the ICT equipment are compliant with the established standards of the government.

²⁹ Electronic Commerce Act of 2000. R.A. 8792. Sec. 11 (b). 2000

PROTECTION OF INDIVIDUALS

The protection of every citizen of the country is primary to the functions of the government. Protection is not only confined to the physical environment but also applies to the cyber environment. To protect the individuals, cybersecurity awareness level must be increased. The government will not be able to combat and address every single adverse event that occurs in a cyber environment. However, when we equip the citizens with the right knowledge and their awareness is increased on cybersecurity, half of the battle is already done. Several projects shall be rolled out as a parallel activity for building up our technical capabilities to protect and secure our cyberspace while we raise the community awareness for cybersecurity.

Accelerate Learning Skills and Development

To implement the strategy for accelerating learning and skills development, there are four (4) objectives that are formulated as bases for developing appropriate programs.

- a. Stimulate the development of approaches and techniques that can rapidly increase the supply of qualified cybersecurity professionals.
 - i. Integration of subjects on cybersecurity in the higher learning curriculum;
 - ii. Integration of cybersecurity in ladderized programs offered by Technical Education and Skills Development Authority (TESDA);

- iii. Promote advanced programs and specialized courses that reduce the time and cost for obtaining knowledge, skills, and abilities for indemand work roles;
- iii.i. Promote the use of interactive learning programs such as webinars
- iv. Encourage the adoption of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills.
- iv.i. Promote apprenticeships and cooperative programs to relevant institution
- b. Promote advanced programs and specialized courses that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles.
 - i. Promote the use of interactive learning programs such as webinars
- c. Encourage the adoption of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills
 - i. Promote apprenticeships and cooperative programs to relevant institution
- d. Promote efforts to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs.

Cybersecurity Outreach Project (QUAD Media for multiplier effect)

Develop strategic relationships with youth organizations, community-based agencies, and relevant private organizations in the domestic and international scene.

- a. #PRinT
 - To develop and activate cybersecurity communication platforms thru Print, Radio, Internet and Television:
 - i. Publication/Blogs/Newspaper
 - ii. Radio – Short ad/Jingle/public service announcements (PSA)
 - iii. Build a strong web presence- Website/Social Media Push/Mobile App
 - iv. Television Plugs - Celebrity Ambassador
- b. Cybersecurity Caravan
- c. National Cybersecurity Awareness Month
- d. Government websites to have cybersecurity related content

National Cybersecurity Awareness Month

Under this strategy, there are five major projects and activities that shall take place until 2022. The goal is to bring the awareness on cybersecurity to a wider audience through these initial project undertaking.

Equipping the Government

- a. Capacity Building for Law Enforcement Agencies
 - i. Judges, Prosecutors
- b. Training of Trainers

Establishment and Creation of Programs for Local and International Cooperation

- a. Establish cooperation and coordination among CERTs and law enforcement (Cybersecurity and Cybercrime, respectively), academia, and industries; and
- b. Formulate and prepare capacity building programs for CERTs and law enforcement

The NCSP shall also provide the guidelines for establishing and creating programs for local and international cooperation. To create a robust cooperation environment, appropriate communications protocol and methods suitable for communicating with the different stakeholders such as the CERTs and the Law Enforcement Agencies, the academe and the industries must be clearly formulated and established. Furthermore, capacity building programs shall be implemented back to back with the cooperation program. The cooperation programs also involve policy issues that can be translated and adopted to the country level, together with the appropriate mechanisms.

ACTIVE APPROACH

Identify

The government has to first establish the baseline as well as understand the business context of the organization's mission critical objectives to ensure that the resources that support the critical functions are provided. There are several of said activities such as Governance, Business Environment, Asset Management, Risk Management Strategy, and Risk Assessment that shall be implemented.

Protect

After identifying and developing organizational understanding to manage cybersecurity risk to the systems, assets, data, industrial controls, and technical capabilities, activities such as Access Control, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology, and Awareness and Training shall be prioritized and included into the execution plan to ensure that the NCSP is implemented.

Detect

The speed and agility of responding to cyberattacks will largely depend on the detection ability and timely discovery of the cybersecurity event. Under this phase, activities such as Anomalies and Events, Security Continuous Monitoring, and Detection Processes are implemented.

Respond

At this juncture, to respond is to develop and implement the appropriate activities regarding a detected cybersecurity event. Under this phase, activities such as Response Planning, Communications, Analysis, Mitigation and Improvements are implemented.

Recover

The recovery stage is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Under this phase, the activities that will cover the implementation plan shall be Recovery Planning, Improvements, and Communications.

PROACTIVE APPROACH

Defend

In developing our defense mechanism, we have to look at how all kinds of physical objects and people are interconnected by way of the ICTs and the internet. The integration of the physical space and the cyberspace are further magnified through the Internet of Things (IoT) phenomenon. Malicious actors in cyberspace are constantly advancing their attack methods. They keep up to date with the latest technological advancement and constantly explore potential gaps within

these new offerings that they can exploit. In the implementation of our defense strategy and to build our defense layers, we must engage every citizen, businesses, organizations, academe, and other governments. This will significantly reduce our exposure to cyberattacks, cyber incidents, or cyber threats and will be able to protect our most valuable assets, while allowing the ability to access, operate successfully, and continuously use the internet. The government's ability to disseminate information must be in a manner and speed appropriate to all types of organization. Timely delivery of information is crucial and important to launch and engage all key stakeholders for a synchronized action to defend our cyberspace and must be simplified.

Deter

In building up the in-depth defense of any government, organization, or enterprise, the first step is to adopt measures that will deter these cyberattacks. There are several actions that can be adopted to serve as deterrence to an attack. One of which is to raise the level of awareness of cybersecurity. We also need to identify these potential threats and anticipate various scenarios to develop countermeasures and use appropriate measures and tools at our disposal. We need to send the message to these malicious actors that they cannot act with impunity. We need to deny our adversaries the opportunity to compromise our systems and networks by trying to understand their intent and capabilities. The LEAs play a critical role in reducing cybercrime. While we harden our CII against cyberattacks and reduce vulnerabilities, the LEA will focus efforts through any technical assistance and data sharing from NCERTs in their relentless pursuit of criminals and cybercriminals.

Develop

The gap between supply and demand for cybersecurity specialists is something that needs to be addressed by the government. In order to address the issue on the supply-demand gap for cybersecurity specialists, an inventory of IT professionals working within the government shall be conducted and specific intervention training programs shall be prepared and developed. Investing into the capacity and capability program should be included in the priority programs. While these short and midterm actions are being implemented, the long term direction shall be on defining and developing the cyber security skills needed across the population. The effort is collaboration among stakeholders from the public sector, academe, and the industry. A review on the Qualification Standards and consultations with the Civil Service Commission, the Department of Budget and Finance and other government agencies shall be conducted to prepare and upgrade the plantilla organization for cybersecurity professionals and specialist who will be recruited for work in the government by making the remuneration package attractive. A Talent Retention Program shall also be planned and prepared for implementation.

METRICS

| Strategic Objectives | Strategic Outcomes | Indicative Success Measures | Contributing to |
|--|---|--|-----------------|
| <p>a. To systematically and methodically harden the Critical Infostructure (CII) for resiliency;</p> | <p>To create a baseline indicators on the resiliency state of the CII</p> | <ul style="list-style-type: none"> • The government is able to establish baseline data that provides details of the state of cybersecurity • Inventory of physical devices and systems in the government and public networks is conducted • Inventory of platforms (such as software and applications) in government and public networks have been conducted • Asset vulnerabilities are identified and documented • Baseline configuration of information technology/ industrial control systems is created and maintained • Audit/log records are determined, documented, implemented and reviewed based on the guidelines (formulated under the NCSP) | <p>Defense</p> |
| <p>b. To prepare and secure government ICT Infostructure (Public and Military);</p> | <p>To reach the desired state of having a resilient CII that can operate during and after cyber-attacks</p> | <ul style="list-style-type: none"> • The government is able to establish a national database e.g. cyber incidences including, Infostructure attacks and intrusions (successful or attempts), etc.) • Lines of communications between government, public, and private sectors are mapped • Resources (such as hardware and software) are prioritized based on their classification: criticality and business value • Response plans (Incident Response and Business Continuity) are in place and managed • Response and recovery plans are tested • Vulnerability management plan is developed and implemented | <p>Protect</p> |

| | | | |
|--|--|--|----------------|
| <p>c. To raise awareness in the business sector on cyber risk and to encourage use of security measures among businesses to prevent and protect, respond and recover from attacks; and</p> | <p>To establish a multi-layer defense, security, and protection in collaboration with the business sector in the event of cyber-attacks</p> | <ul style="list-style-type: none"> • Conduct a catalogue of external information systems • Sharing forums and sources are established on threat and vulnerability information • Events are reported and information is shared, which is consistent with the response plan • Voluntary information sharing occurs with external stakeholders to achieve broader situational awareness | <p>Detect</p> |
| <p>d. To raise awareness of individuals on cyber risks among users as they are the weakest links who need to adopt the right norms in Cybersecurity.</p> | <p>To increase awareness on cybersecurity and widen the reach for internet users which will lessen the entry point into the network systems of the government, public, and private networks of perpetrators and attackers.</p> | <ul style="list-style-type: none"> • Vulnerable sectors in the society (such as the youth and small and medium sized business owners) shall be prioritized for awareness on cybersecuritymanagement plan is developed and implemented | <p>Protect</p> |

CONCLUSION

CyberSecurity is an evolving field with many international actors at play. As such, it is imperative that a reliable mechanism is in place to address constant updates in the virtual arena, underpinned on the premise of collaboration with allied countries in the fronts of knowledge sharing, coarchitecture of laboratories/training facilities, and mobility exchange.

In line with this, to keep abreast with the latest trends, a capacity building program of international standard must be set in place in accordance to the demands of digital forensics, network analytics, and defense conceptualization, among others. Included in the cooperation are detection/mitigation regimes, frameworks for coordination of international originators of attacks, and co-design of stakeholder engagement strategies.

Admittedly, the Philippines' state of cybersecurity is still at its infancy stage, even though there have been previous initiatives that have already been undertaken through different agencies, including enabling of the laws that have been promulgated to protect data and information. The NCSP 2022 shall provide the roadmap to make a coherent and cohesive strategy for cybersecurity and act as the enabler for institutionalizing all the initiatives and strategies that have already been started by different government agencies. Furthermore, it will address the issue and challenges of a synchronized defense in the event of an attack because the roles, functions, objectives and goals are clear and well defined. We need to be ready for the disruptive nature that technology brings. This is amplified further by the threats of cyberattacks and disruption of systems (mechanical or human errors), whether accidental or deliberate. We need to work as one in order to combat the challenges that are posed by the dynamic and fluid changes that occur in cyberspace as technology evolves and interconnectivity cuts across all levels of government and society.

GLOSSARY

Access refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.

Communication refers to the transmission of information through information and communication technology (ICT) media, including voice, video and other forms of data.

Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.

Computer data refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system. including a program suitable to cause a computer system to perform a function, and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

Computer program refers to a set of instructions executed by the computer to achieve intended results.

Critical infrastructure refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data 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.

Cyber refers to a computer or a computer network, the electronic medium in which online communication takes place.

Cyber espionage refers to the use of computer networks to gain illicit access to confidential information, typically that by a government or other organization.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

Cybersecurity refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

Cyberspace used to describe virtual world of computers.

Database refers to a representation of information, knowledge, facts, concepts or instructions which are being prepared, processed or stored, or have been prepared, processed or stored in a formalized manner, and which are intended for use in a computer system.

Distributed Denial of Service (DDoS) is an attack in which multiple compromised computer systems attack a target, such as a server, website, or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests, or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

Internet of things (IoT) a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

Law Enforcement Authorities (LEAs) refers to the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) under section 10 of RA 10175.

Malware short for "malicious software," refers to software programs designed to damage or do other unwanted actions on a computer system.

National CyberSecurity Plan (NCSP) refers to a comprehensive plan of actions designed to improve the security and enhance cyber resilience of infrastructures and services. It is a top-down approach to cybersecurity that contains broad policy statements and establishes a set of national objectives and priorities that should be achieved within a specific timeframe.

National Security System (NSS) means any information system (including telecommunication system) used or operated by any organization or outsourced to a third party.

Phishing is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, Social Security numbers, or other sensitive personal information. The spoofed e-mail message urges the recipient to click on a link to update their personal profile or carry out some transaction. The link then takes the victim to a fake website where any personal or financial information entered is routed directly to the scammer.

Preservation refers to the keeping of data that already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. It is the activity that keeps that stored data secure and safe.

Traffic Data or Non-Content Data refers to any computer data other than the content of the communication, including but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

RODOLFO A. SALALIMA SECRETARY



Secretary Rodolfo Salalima is currently the Secretary of the Department of Information and Communications Technology (DICT). He is a man with extensive experience in IT both in the Philippines and on the international front. His over 40 years of legal experience in the field of broadcast and telecommunications industry led him to hold various executive positions in the telecommunications sector, both local and international, such as Telecommunications and Broadcast Attorneys of the Philippines Inc., the Philippine Electronics, and Telecommunications Federations in 1992 to 1996. He also served as Vice Chairman of the International Telecommunication Union (ITU) Council Working Group that worked on the Amendment of the ITU Constitution and Convention at Geneva, Switzerland.

Secretary Salalima was appointed by President Rodrigo Duterte as the first Secretary for the newly established Department of ICT in 2016 where he committed to leave a lasting legacy of enabling a one digitized government and empowering the Filipinos through ICT.



ELISEO M. RIO, JR. UNDERSECRETARY FOR SPECIAL CONCERNS

Undersecretary Eliseo M. Rio, Jr. was appointed as Undersecretary for Special Concerns of the DICT last September 13, 2016. He is an Electronic and Communications Engineer who left an indelible mark in the field as the fourth placer in the first Philippine ECE Licensure in 1971 and the “Most Outstanding Professional in the Field of Electronics and Communication for the Year 2002.”

He served the Armed Forces of the Philippines (AFP) where he held various positions and retired as a Brigadier General. He was also a former Commissioner at the National Telecommunications Commission (NTC) where one of his significant accomplishments was surfacing the way to the proliferation of Call Centers and BPOs by enacting NTC MC 08-07-2002 or the Rules and Regulations Authorizing Entities Other than Public Telecommunications Entities to Install and Operate Public Calling Stations/Offices and Telecenters in 2002.



MONCHITO B. IBRAHIM UNDERSECRETARY FOR OPERATIONS AND MANAGEMENT

Undersecretary Mon Ibrahim was appointed as Undersecretary for Operation and Management last March 2017. His extensive IT career which started in 1975 has seen him working for multinational companies like Fujitsu, WeServ, Siemens-Nixdorf, Comparex Germany, and Unisys Australia in various executive positions.

He served as a member of the Executive Committee of the Southeast Asia Regional Computer Confederation from 2004 to 2005, the Board of Advisers of the De La Salle University College of Computer Studies, and the University of the Philippines Information Technology Development Center (UPITDC). Currently, he is a Trustee and President of the University of the Philippines System Information Technology Foundation (UPSITF) and serving his 9th term as member of the Technical Panel for Information Technology Education (TPITE) of the Commission on Higher Education (CHED).

He finished his B. S. Major in Chemistry at the Far Eastern University and attended Ateneo de Manila University Graduate School of Business for his post graduate studies. He also completed a Public Sector Executive Program on Innovative Government at the Lee Kuan Yew School of Public Policy of the National University of Singapore.



DENIS F. VILLORENTE UNDERSECRETARY FOR INNOVATIONS AND DEVELOPMENT

Prior to his stint as Undersecretary for the DICT, Usec. Villorente served as Deputy Executive Director for e-government at the Information and Communications Technology Office (ICTO) where he conceptualized the Integrated Government Philippines (iGov) Project, a comprehensive program that aims to connect government agencies through shared infrastructure and ICT services. He was also Director of the Advanced Science and Technology Institute, an agency under the Department of Science and Technology, where he was instrumental in the establishment of the Philippine Open Internet Exchange (PHOpenIX).

Undersecretary Villorente is a graduate of the University of the Philippines' College of Engineering.



ALLAN S. CABANLONG
**ASSISTANT SECRETARY FOR CYBERSECURITY
 AND ENABLING TECHNOLOGIES**

Assistant Secretary for Cybersecurity and Enabling Technologies for the DICT and concurrent Executive Director for Cybercrime Investigation and Coordination Center Allan Salim Cabanlong is an ASEAN Engineer, a Professional Electronics Engineer, and a graduate of Masters of Science in Global Information and Telecommunications Studies at the Waseda University in Tokyo, Japan. He was instrumental in the passage of the Cybercrime Prevention Act of 2012 and his expertise in the field of ICT also helped him author books published internationally namely: “Law, Policy and Technology: Cyber Terrorism, Information Warfare and Internet Immobilization” published in 2012; and “Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity in European Journal of Law and Technology” in 2010.

Assistant Secretary Cabanlong is a recipient of various local and international awards and has served the Philippine National Police as Chief of Web Services and Cybersecurity Division and Chief of the Information Technology Office prior to his appointment as Assistant Secretary in the DICT.

He is also a recognized global expert in the field of cybersecurity and the leading figure in the crafting of the Philippine National Cybersecurity Plan 2022.

ALAN A. SILOR
ASSISTANT SECRETARY



Assistant Secretary Silor is a proud son of Butuan City in Mindanao. He has done extensive work with ICT-related NGOs and has served in leading business organizations in various capacities. He is a member and former President of the Butuan City Chamber of Commerce and Industry, Vice President for Business and Government Affairs of the Filipino-Chinese Chamber of Commerce of Agusan, and a member of the Institute of Electronics Engineers of the Philippines. Asec. Silor has also worked as a station manager for two local stations in Butuan, was a President of the Caraga ICT Council, and was part of the Audit and Standards Authority of the Kapisanan ng mga Brodkaster ng Pilipinas.

Assistant Secretary Alan Silor’s current focus is the DICT project monitoring and implementation in the various regions of the country.

CARLOS MAYORICO E. CALIWARA
**ASSISTANT SECRETARY FOR LEGAL AFFAIRS AND
 COMMUNICATIONS AND CHIEF OF STAFF OF THE
 SECRETARY**



Assistant Secretary Caliwara supervises the legal affairs and communications unit of the DICT and also functions as the Chief of Staff to the Secretary of ICT. Asec. Caliwara has been with the ICT industry since the early 1990s. He served as legal counsel for various local and international companies, dealing with ICT-related issues in contract management, human resources, intellectual property management, and information security management. Atty. Caliwara is a staunch advocate of the protection of Filipino intellectual property works and digital piracy. He started working as a consultant to ICTO’s Free WiFi in Public Places Project where he closely worked with the project team on legal and technical matters.

Assistant Secretary Caliwara graduated from the Far Eastern University with a degree in A.B. Political Science and secured Law degree from the San Beda College of Law. He also has a Diploma in Industrial Relations from the University of the Philippines.

JOHN HENRY D. NAGA
ASSISTANT SECRETARY



Assistant Secretary Naga currently handles DICT’s legislative liaison, general management, and the development and implementation of the merit and selection plan. Atty. Naga’s major accomplishment in the field of ICT is his pioneering work in the conversion of all GMA TV Stations from analog TV to Digital Terrestrial Television Broadcast.

Atty. Naga is a graduate of the San Beda College of Law, and has worked as a lawyer in the fields of telecommunications, broadcast media, government and corporate contracts, corporate legal management, and labor relations.