Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
First Regular Session

HOUSE BILL NO. 7057

Introduced by **ANG PROBINSYANO**
Party-List Representative Alfred Delos Santos

EXPLANATORY NOTE

Cyberspace, compared to conventional physical space, is particularly difficult to secure. First, malicious and sophisticated actors can launch a wide range of threats and hazards, both physical and cyber, and operate anywhere in the world. State and non-state actors exploit the vulnerabilities in the information and communications technology (ICT) frameworks to steal information and money and are further developing capabilities to damage, sabotage, and terrorize societies, specifically the delivery of crucial services.

Second, the increasing shift and dependence on cyber networks to provide services have posed compounded vulnerabilities and weaknesses. As a result, it leads to more intertwined cyberspace and critical underlying infrastructure which is subject to risks for wide-scale critical attacks that could cause harm and disrupt services, eventually paralyzing our economy and the lives of millions of Filipinos, specifically the marginalized sectors.

The Philippines has been subject to cybercrime attacks including hacking and identity theft, both in the government and in private institutions. For example, the 2016 hacking of COMELEC has released sensitive and personal information to the public. In the same year, 68 government websites were attacked after the release of the Permanent Court of Arbitration's (PCA) ruling on the West Philippine Sea issue. Throughout the years, we have witnessed an increasing number of cyber-attacks and has put the Philippines on the top list in terms of cyber-attacks and threats.

In light of the increasing number of risks and potential effects of such cyber events and a demand to have a more capable defense and security which can respond to these threats, strengthening the security and resilience of our cyberspace is the main task that needs to be promptly acknowledged.

As a proactive and institutionally cohesive response, this bill aims to establish a national agency primarily tasked to implement cybersecurity measures and protect linked infrastructure in order to enhance further the delivery of services and increase trust and confidence in the government with transactions concerning sensitive and personal information. Creating a single body to address this national concern will prove to capacitate and move the cybersecurity agenda forward.

In this regard and the whole of the Filipino nation in mind, I look forward to the passage of this Bill.

ALFRED C. DELOS SANTOS
Representative, Ang Probinsyano Partylist

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
First Regular Session

HOUSE BILL NO. 7057

Introduced by **ANG PROBINSYANO**
Party-List Representative Alfred Delos Santos

AN ACT INSTITUTING THE CYBERSECURITY AND INFRASTRUCTURE PROTECTION ACT OF 2020

Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled:

SECTION 1. *Short Title.* – This Act shall be known as the "Cybersecurity and Infrastructure Protection Act of 2020."

SECTION 2. *Declaration of Policy.* – Article II, Section 4 of the 1987 Constitution states:

> "The prime duty of the Government is to serve and protect the people..."

Towards this end, the State shall endeavor in programs that protect the rights and interests of the people, especially that which considers security. The State shall take necessary measures in order to ensure that the services provided are not impeded and overall welfare and well-being in both the physical and cyberspace safeguarded.

Equally, Article XIV, Section 10 of the same Constitution provides:

> "Science and technology are essential for national development and progress. The State shall give priority to research and development, invention, innovation, and their utilization; and to science and technology education, training, and services. It shall support indigenous, appropriate, and self-reliant scientific and technological capabilities, and their application to the country's productive systems and national life."

The State recognizes the role of science and technology in ensuring the protection of the people especially with threats within cyberspace. Towards this end, the State shall invest in programs that will address future threats and build scientific capabilities and self-reliance in cybersecurity.

SECTION 3. *Objectives.* – The objectives of this Act are as follows:

a. To recognize the increasing importance of establishing an agency that is tasked in improving cybersecurity and infrastructure protection considering threats and security concerns within cyberspace;
b. To improve Information and Communication Technology (ICT) frameworks in order to enhance the delivery of services;
c. To protect the information of the State and its citizens and build on the national capacity to defend against cyber threats and acts of terrorism;
d. To invest and capacitate our own personnel to respond to the growing need to establish a renowned and self-reliant cybersecurity agency; and
e. To consolidate existing efforts to protect the State's cyber interest and effectively implement the National Cybersecurity Plan.

SECTION 4. *Definition of Terms.* – For the purposes of this Act, the following definitions shall apply:

a. Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;
b. Computer system refers to an arrangement of interconnected computers that are designed to perform one or more specific functions, and includes —
    i. an information technology system; and
    ii. an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;
c. 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 are so vital to the state that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on national or economic security, national public health, and safety, or any combinational of those matters.

d. Cybersecurity refers to the state in which a computer or computer system is protected from unauthorized access or attack;
e. Cybersecurity incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardizes or adversely affects its cybersecurity or the cybersecurity of another computer or computer system;
f. Cybersecurity program refers to any computer program designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of a computer or computer system;
g. Cybersecurity threat refers to an act or activity (whether known or suspected) carried out on or through a computer or computer system, that may imminently jeopardize or affect adversely, without lawful authority, the cybersecurity of that or another computer or computer system;

SECTION 5. *Cybersecurity and Infrastructure Protection Commission.* – There is hereby created the "Cybersecurity and Infrastructure Protection Commission", hereinafter referred to as the "Commission". The Commission shall be independent and autonomous and shall have the same status as that of a national government agency attached to the Office of the President. It shall be headed by the Cybersecurity Commissioner.

SECTION 6. *Duties and Responsibilities.* – The Commission shall have the following duties and functions:

a. oversee and promote the cybersecurity of computers and computer systems in the Philippines;
b. to advise the Government or any other public authority on national needs and policies in respect of cybersecurity matters generally;
c. to monitor cybersecurity threats, whether such cybersecurity threats occur in or outside the Philippines;
d. to respond to cybersecurity incidents that threaten the national security, defense, economy, foreign relations, public health, public order or public safety, or any essential services, of the Philippines, whether such cybersecurity incidents occur in or outside the Philippines;
e. to identify and designate critical infrastructure, and to regulate owners of critical infrastructure with regard to the cybersecurity of the critical infrastructure;
f. to represent the Government on cybersecurity issues internationally;
g. to cooperate with cyber emergency response teams (CERTs) of other countries or territories on cybersecurity incidents;
h. to establish standards within the Philippines in relation to cybersecurity products or services, and the recommended level of

cybersecurity of computer hardware or software, including certification or accreditation schemes;

i. to promote, develop, maintain and improve competencies and professional standards of persons working in the field of cybersecurity;
j. to support the advancement of technology, and research and development relating to cybersecurity;
k. to promote awareness of the need for and the importance of cybersecurity in the Philippines.
l. to aid for further implementation of other cyber laws such as, but not limited to:
    i. Republic Act 10175, otherwise known as the "Cybercrime Prevention Act of 2012"
    ii. Republic Act 8792, otherwise known as the "E-Commerce Act of 2000"
    iii. Republic Act 10173, otherwise known as the "Data Privacy Act of 2012"

SECTION 7. *Cybersecurity Commissioner.* – There shall be one (1) "Cybersecurity Commissioner", hereinafter referred to as the "Commissioner". The Commissioner shall be a natural-born citizen of the Philippines; have occupied positions of responsibility and leadership in information and communications technology (ICT) organizations or institutions; of good moral character; and not have been convicted of any crime involving moral turpitude. The Commissioner shall serve as the head and official representative of the Commission and shall oversee the overall implementation of this Act.

SECTION 8. *National Cybersecurity Plan and Framework.* – There shall be created a National Cybersecurity Plan which aims to address the cybersecurity threats and create measures that will lead to a secure and resilient Philippine cyberspace. It shall be the institutional framework and foundation that shall be implemented by the Commission, together with other partner agencies involved in cybersecurity.

Further, the National Cybersecurity Plan and Framework shall include, but not limited to:

1. Cybersecurity Assessment and Compliance
2. National Cybersecurity Drills and Exercises
3. National Database for Monitoring and Reporting
4. Cybersecurity Enhancement Programs in Government Agencies and Local Government
5. Threat Intelligence and Analysis Program
6. Basic Cyber Emergency Response Program
7. National Common Information and Communications Technology (ICT) Equipment Security Evaluation and Certification Project

8. Update of Cybersecurity Software Licenses
9. Installation of Cybersecurity Hubs
10. Protection of Electronic Government (e-Gov) Services and Transactions

SECTION 9. *National Cyber Emergency Response Protocol.* – There shall be an established National Cyber Emergency Response Protocol, hereinafter referred to as "Protocol". The Commission, in coordination with the Advisory Council, shall formulate the Protocol to aid government agencies, sectors, and organizations in the event of cybersecurity incidents or cybersecurity threats.

SECTION 10. *Capacity Building and Capability Development.* – The government, through the Commission, shall endeavor to invest in capacity building, capability development programs, competitive staff remuneration, cyber training facilities, and cybersecurity and research development. The Commission shall engage and collaborate with the academe and other institutions to support the development of cybersecurity specialists through collaboration and development.

Further, the Commission, in the interest of developing qualified and competent cybersecurity professionals, shall provide for scholarships for training and development through short executive courses or postgraduate degree programs.

SECTION 11. Advisory Council. – There shall be an Advisory Council which shall be composed of the Secretary of the Department of Information and Communications Technology (DICT), as Chairman, and the Secretaries of Department of Justice (DOJ), Department of Science and Technology (DOST), Department of National Defense (DND), Department of Interior and Local Government (DILG), Director-General of the National Security Council, Chief of the Philippine National Police, Director of the National Bureau of Investigation (NBI), and the Chairperson of both Senate and House Committees dealing with security and technology.

The Council shall meet once every three (3) months, or as often as may be necessary, upon the call of its chairman, advise and be consulted by the Commission on important matters relating to cybersecurity, infrastructure protection, and development.

The Council may form task forces which shall convene between the meetings of the Council. The Commission shall provide the technical support required by the Council to function according to this Act.

SECTION 12. *Appropriations.* – An initial fund of P500 million shall be appropriated for the immediate implementation of this Act. Thereafter, such sums as may be necessary for the continued operations and maintenance of the programs shall be included in the annual General Appropriations Act.

SECTION 13. *Separability Clause.* – If any provision or part of this Act is held invalid or unconstitutional, the remaining provisions or parts unaffected shall remain in full force and effect.

SECTION 14. *Repealing Clause.* – All laws, executive orders, presidential decrees or issuances, letters of instruction, administrative orders, rules, and regulations contrary to or inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SECTION 15. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,