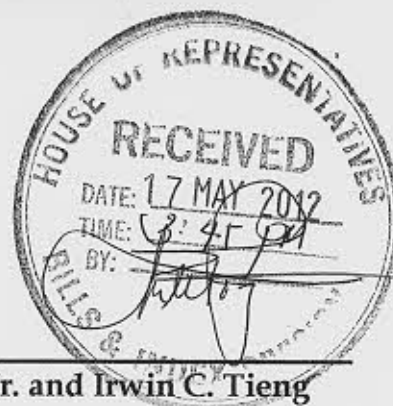


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

FIFTEENTH CONGRESS
Second Regular Session

House Bill No. 6200



Introduced by Representatives Mariano Michael M. Velarde Jr. and Irwin C. Tieng
(BUHAY Party List)

EXPLANATORY NOTE

Presently there are two (2) cybercrime bills pending approval, e.g., Senate Bill no. 2796 AN ACT DEFINING CYBERCRIME, PROVIDING FOR PREVENTION, INVESTIGATION AND IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES which has passed the third reading and House Bill No. 5808 AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES which is presently being considered in second reading.

However, said bills define and penalizes cybercrime in general and specifically on economic and social crimes. The intent of the current bill is to address cyber terrorism or terrorist acts committed in cyberspace. Cyber terrorism is generally understood to mean unlawful attacks and threats to attack against computers, networks, and the information stored therein and when done to intimidate or coerce a government or its people in furtherance of political or ideological objectives.

Terrorism as a politically or ideologically motivated criminal act has been a growing concern and menace that haunts the national and international communities since such acts can be transnational in operation and effect. As technology develops, terrorist capability improves and government has to cope up with.

The February denial-of-service attacks against Yahoo, CNN, eBay, and other e-commerce Web sites was estimated to have caused over a billion in losses. It also shook the confidence of business and individuals in e-commerce. The recent defacement of some government websites has caused concern and inconvenience to government and to the public.

The passage of this bill is hereby earnestly sought.

Republic of the Philippines
House of Representatives
Quezon City

15th CONGRESS
2nd Regular Session

House Bill No. 6200

Introduced by Rep. Mariano Michael M. Velarde Jr. and Rep. Irwin C. Tieng

**AN ACT DEFINING AND CRIMINALIZING CYBER TERRORISM IN
THE PHILIPPINES**

Be it enacted by the Senate and HOUSE OF REPRESENTATIVES of the Philippines in Congress assembled:

SECTION 1. *Title.* - This Act shall be known as the "*Anti Cyber Terrorism Bill of 2012.*"

SEC. 2. *Declaration of Policy.* - The State recognizes the increasingly vital role of information and communications technology (ICT) as an enabler of key industries, such as banking, broadcasting, business process outsourcing, electronic commerce, and telecommunications, and as a driving force for the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and application of ICT to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer and communications systems, networks, and database, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making such conduct punishable under the law. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

SEC. 3 *Definition of Terms.* - For purposes of this Act, the following terms are hereby defined as follows:

- (a) *Access* - refers to the instruction, communication with, storage of data in, retrieval of data from, or otherwise making use of any resource of a computer system;
- (b) *Alteration* - refers to the modification or change, in form or substance, of an existing computer data or program;
- (c) *Communication* - refers to the transmission of information, including voice and non-voice data;

- (d) *Computer attack* – refers to any action directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data;
- (e) *Computer system* – refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities, including but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media;
- (f) *Computer Data* – refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system, including any program capable of causing a computer system to perform a function, as well as electronic documents or electronic data messages;
- (g) *Computer Program* – refers to a set of instructions executed by the computer to achieve intended results;
- (h) *Conduct Without Right* – refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law;
- (i) *Cyber Terrorism* – refers to a terrorist act that disrupts information systems: the use of techniques that disrupt or damage computer-based information systems to cause fear, injury, or economic loss. It could mean attacks and threats of attack against computers, networks, computer systems, computer programs, and data and the information stored therein; and done to intimidate or coerce a government or its people in furtherance of political or social objectives; and which result in violence against persons or property, or at least cause enough harm to generate fear.
- (j) *Cyberterrorist*– refers to a programmer who breaks into computer systems in order to steal or change or destroy information as a form of cyber-terrorism;
- (k) *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 an organized manner and which are intended for use in a computer system;
- (l) *E-mail Bombing* – refers to the repeated sending of huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack;
- (m) *E-mail Spamming* – refers to the sending of email to hundreds or thousands of users (or to lists that expand to that many users; it can be made worse if recipients reply to the email, causing all the original addressees to receive the reply;
- (n) *Hacking* – means finding out weaknesses in a computer, computer system or computer network and exploiting them;
- (o) *Interception* – refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the content of data, either directly, through access

and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

(p) *Service Provider* – refers to: (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(q) *Subscriber's Information* – refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (i) the type of communication service used, the technical provisions taken thereto and the period of service; (ii) the subscriber's identity, postal or geographic address, telephone and other access number, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; (iii) any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

(r) *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;

(s) *Virus Attack* – refers to the launching or release of malicious wares such as viruses, worms, file infectors, and similar destructive wares.

CHAPTER II – PUNISHABLE ACTS

SEC. 4. *Cyber Terrorism Offense*: The following acts constitute the offense of Cyber Terrorism punishable under this Act:

A. *Cyberterrorist attacks* – serious attacks directed against critical computer infrastructures which result to explosions, plane crashes, water contamination, and similar incidents leading to death and/or bodily injury or severe economic loss;

B. *Computer Attacks* – any action directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data resulting to defacement of websites with political and social messages or Denial-of-Service (DoS) attacks – disrupting access to target websites, usually by flooding them with traffic. It may be done through any of the following methods:

(i) *Physical attack (PA)* which involves the use of conventional weapons against a computer facility or its transmission lines;

(ii) *Electronic attack (EA)* which involves the use the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; or

(iii) *Computer network attack (CNA)*, usually involves the use of malicious code as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CNA are enabled when an attacker uses stolen information to enter restricted computer systems;

C. Virus Attack – launching or release of malicious wares such as viruses, worms, file infectors, and similar wares

D. E-mail Bombing – the repeated sending of huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack;

E. E-mail Spamming – the sending of email to hundreds or thousands of users or to lists that expand to that many users and which is made worse if recipients reply to the email, causing all the original addressees to receive the reply;

F. Hacking – the act of finding out weaknesses in a computer, computer program computer system or computer network and exploiting them to cause damage to that computer program, system or network;

SEC. 5. *Other Offenses*. The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of cyberterrorist offense– any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable; or

(b) Attempt to Commit cyberterrorist offense– any person who willfully attempts to commit any of offenses enumerated in this Act shall be held liable.

SEC. 6. *Liability under Other Laws*. A prosecution under this Act shall be without prejudice to any liability for violation of any provision of Republic Act No. 3815, as amended, otherwise known as the Revised Penal Code, or any other law.

CHAPTER III – PENALTIES

SEC. 7. *Penalties*. – The following penalties shall be imposed on violations under this Act:

(a) Any person found guilty of any of the punishable acts enumerated in Section 4 (A), (B) and (C) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (PhP 200,000.00) up to a maximum amount commensurate to the damage incurred or both.

(b) Any person found guilty of any of the punishable acts enumerated in Section 4 (D), (E) and (F) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Five Hundred Thousand Pesos (PhP 500,000.00) up to a maximum amount commensurate to the damage incurred or both.

(c) Any person found guilty of any of the punishable acts enumerated in Section 5 of this Act shall be punished with imprisonment of *arresto mayor* or a fine of at least One Million Pesos (PhP 1,000,000.00) up to a maximum amount commensurate to the damage incurred or both.

SEC. 8. *Corporate Liability.* – When any of the punishable acts herein defined is knowingly committed in behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power representation of the juridical person; (b) an authority to take decision on behalf of the juridical person; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten Million Pesos (PhP10,000,000.00).

When the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five Million Pesos (Php 5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION

SEC. 9. *Law Enforcement Agencies* – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall designate special investigators to exclusively handle cases involving violations of this Act.

SEC. 10. *Real-time Collection of Computer Data.* – Law enforcement authorities shall be authorized to collect or record by technical or electronic means, and service providers are required to collect or record by technical or electronic means, and/or to cooperate and assist law enforcement authorities in the collection or recording of, traffic data, in real-time, associated with the specified communications transmitted by means of a computer system, subject to existing laws and procedures.

SEC. 11. *Preservation of Computer Data.* – The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved up to a minimum period of six (6) months from the date of the transaction. Content data shall be preserved for a minimum period of six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension of six (6) months: Provided, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

SEC. 12. *Disclosure of Computer Data* – Law enforcement authorities shall be authorized to issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for investigation purposes.

SEC.13. *Search, Seizure and Examination of Computer Data.* – Where a search and seizure warrant is properly issued, law enforcement authorities shall, within the time period specified in the warrant, have the following powers and duties:

- (a) To conduct interception, as defined in this Act, of content data;
- (b) To secure a computer system or a computer-data storage medium;
- (c) To make and retain a copy of secured computer data;
- (d) To maintain the integrity of the relevant stored computer data;
- (e) To conduct examination of the computer data storage medium; and
- (f) To render inaccessible or remove those computer data in the accessed computer system.

The law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of expiration of the warrant.

CHAPTER V – JURISDICTION

SEC.14. *Jurisdiction.* – The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act committed within the territory of the Philippines, including Philippine ships or airships, or by a Filipino national regardless of the place of commission. Jurisdiction shall also cover any of the elements committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission, any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

The Department of Justice (DOJ) shall designate special prosecutors to exclusively handle cases involving violations of this Act.

CHAPTER VI – INTERNATIONAL COOPERATION

SEC. 15. *Mutual Assistance and Cooperation.* – The Government of the Philippines shall cooperate with, and render assistance to other nations for purposes of detection, investigation, and prosecution of offenses referred to in this Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree 1069, otherwise known as the Philippine Extradition Law and other pertinent laws shall apply.

In this regard, the Government of the Philippines shall:

(1) Provide assistance to a requesting nation in the real-time collection of traffic data associated with specified communications in the Philippine territory transmitted by means of a computer system, with respect to criminal offences defined in this law for which real-time collection of traffic data would be available;

(2) Provide assistance to a requesting nation in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system to the extent permitted under Republic Act No. 4200, otherwise known as the Anti Wiretapping Act, Republic Act No. 9372, otherwise known as the Human Security Act of 2007, and other related and pertinent laws;

(3) Allow another nation, without its authorization to:

(a) access publicly available stored computer data, located in Philippine territory, or elsewhere; or

(b) access or receive, through a computer system located in Philippine territory, stored computer data located in another country, if the nation obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the nation through that computer system;

(4) Entertain a request of another nation for it to order or obtain the expeditious preservation of data stored by means of a computer system, located within Philippine territory, relative to which the requesting nation intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(a) A request for preservation of data under this Section shall specify:

(i) the authority seeking the preservation;

(ii) the offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(iii) the stored computer data to be preserved and its relationship to the offence;

(iv) the necessity of the preservation; and

(v) that the requesting nation intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(b) Upon receiving the request from another nation, the Government of the Philippines shall take all appropriate measures to preserve expeditiously the specified data in accordance with this law and other pertinent laws. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

(c) A request for preservation may only be refused if:

(i) the request concerns an offense which the Government of the Philippines considers as a political offense or an offense connected with a political offense; or

(ii) the Government of the Philippines considers the execution of the request will prejudice its sovereignty, security, public order or other national interest.

(d) Where the Government of the Philippines believes that preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting nation's investigation, it shall promptly so inform the requesting nation. The requesting nation will determine whether its request should be executed.

(e) Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting nation to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request the data shall continue to be preserved pending a decision on that request.

(5) Accommodate request from another nation to search, access, seize, secure, or disclose data stored by means of a computer system located within Philippine territory, including data that has been preserved under the previous subsection. The Government of the Philippines shall respond to the request through the proper application of international instruments, arrangements and laws.

(a) The request shall be responded to on an expedited basis where:

(i) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

(ii) the instruments, arrangements and laws referred to in number 2 of this Section otherwise provide for expedited co-operation.

(b) The requesting nation must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the request information subject to the conditions specified in the grant.

SEC. 16. *Grounds for Refusal to Cooperate.* – The Government of the Philippines shall have the right to refuse cooperation under any of the following grounds:

(a) the offense is punishable under Philippine laws and the Philippine courts have acquired jurisdiction over the person of the accused;

(b) the information requested is privileged, protected under Philippine laws, or that which affects national security;

(c) if, for any reason, the production of the information is unreasonable,

(d) the foreign government requesting for assistance has previously refused without justifiable reason, a similar request by the Government of the Philippines; and

(e) the foreign government requesting for assistance has previously breached an agreement to keep the fact or subject of request confidential, or has previously violated any condition of the grant.

SEC. 17. *Cooperation Based on Reciprocity.* — In the absence of a treaty or agreement, mutual assistance and cooperation under the preceding sections in this Chapter shall be based on the principle of reciprocity.

CHAPTER VII – FINAL PROVISIONS

SEC. 18. *Appropriations.* — The amount necessary to implement the provisions of this Act shall be included in the Annual General Appropriations Act.

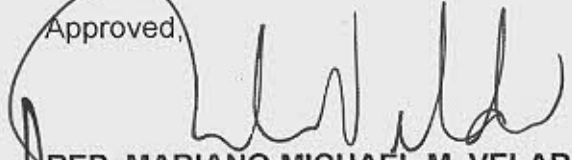
SEC. 19. *Implementing Rules and Regulations.* — The Commission on Information and Communications Technology (CICT) and the Department of Justice shall jointly formulate the necessary rules and regulations for the effective implementation of this Act.

SEC. 20. *Separability Clause.* — If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

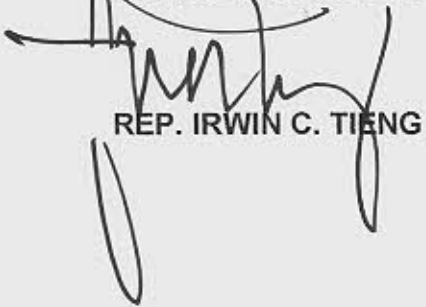
SEC. 21. *Repealing Clause.* — All laws, decrees, or rules inconsistent with this Act are hereby repealed or modified accordingly. Specifically, Section 33 of Republic Act No. 8792 or the Electronic Commerce Act is hereby modified accordingly.

SEC. 22. *Effectivity.* — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in at least two (2) newspapers of general circulation,

Approved,



REP. MARIANO MICHAEL M. VELARDE Jr.



REP. IRWIN C. TIENG