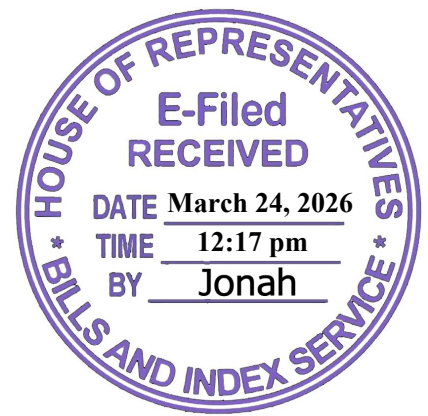


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS
First Regular Session

House Bill No. 8753



Introduced by: **REPRESENTATIVE ERIC L. OLIVAREZ**

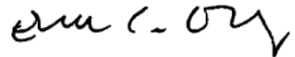
EXPLANATORY NOTE

The Philippines faces evolving national security threats arising from espionage, cyber-espionage, and unauthorized foreign intelligence activities targeting government institutions, defense systems, critical infrastructure, and strategic industries. Advances in digital technology and global connectivity have expanded the methods by which hostile actors may infiltrate computer networks, compromise communications systems, and obtain sensitive national defense information.

While existing laws such as Commonwealth Act No. 616 (Espionage Act) and Republic Act No. 10175 (Cybercrime Prevention Act of 2012) address certain aspects of espionage and cybercrime, these statutes were enacted in vastly different technological contexts and do not fully address the complex and coordinated intelligence operations that may now occur through cyberspace, research institutions, and critical digital infrastructure.

This measure seeks to strengthen the State's capacity to prevent, detect, investigate, and prosecute espionage and cyber-espionage by establishing a comprehensive legal framework that protects classified national defense information, secures critical information infrastructure, and deters foreign intelligence operations directed against the Republic of the Philippines, while ensuring that enforcement remains consistent with the Constitution and respectful of civil liberties.

In view of the foregoing, the passage of this measure is earnestly sought.


ERIC L. OLIVAREZ

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS

First Regular Session

House Bill No. 8753

Introduced by: **REPRESENTATIVE ERIC L. OLIVAREZ**

**“AN ACT
STRENGTHENING NATIONAL DEFENSE AGAINST
ESPIONAGE, CYBER-ESPIONAGE, AND UNAUTHORIZED
FOREIGN INTELLIGENCE ACTIVITIES; PROTECTING
CLASSIFIED GOVERNMENT INFORMATION AND CRITICAL
INFORMATION INFRASTRUCTURE; ESTABLISHING A
NATIONAL FRAMEWORK FOR COUNTER-ESPIONAGE AND
CYBER-INTELLIGENCE DEFENSE; PRESCRIBING PENALTIES
FOR VIOLATIONS; AND FOR OTHER PURPOSES”**

Section 1. Short Title. — This Act shall be known as the “National Espionage and Cyber-Intelligence Defense Act of 2026.”

**ARTICLE I.
DECLARATION OF POLICY**

Section 2. Declaration of Policy. — It is hereby declared the policy of the State to:

- a. Protect the sovereignty, territorial integrity, and national security of the Republic of the Philippines;
- b. Safeguard critical communication infrastructure, digital networks, military systems, and strategic industries from espionage, cyber intrusion, sabotage, and foreign intelligence operations;
- c. Strengthen the ability of the State to detect, prevent, investigate, and prosecute acts of espionage whether conducted through physical infiltration, cyber intrusion, or technological means;
- d. Protect sensitive national defense information, critical infrastructure data, and government communications from unauthorized acquisition, hacking, or disclosure;
- e. Ensure that measures undertaken pursuant to this Act are implemented consistent with the Constitution and with due respect for civil liberties, academic freedom, and freedom of expression.

ARTICLE II

DEFINITION OF TERMS

Section 3. Definitions. — For purposes of this Act:

- a. Espionage — Refers to the act of knowingly obtaining, collecting, transmitting, delivering, or communicating information relating to national defense, critical infrastructure, intelligence operations, or government security to a foreign state, foreign intelligence entity, or foreign agent with intent or reason to believe that such information will be used to injure the national security of the Republic of the Philippines or to the advantage of a foreign state.
- b. Cyber Espionage — Refers to intentional and unauthorized access to computer systems, communications networks, satellites, or digital infrastructure for the purpose of obtaining classified national defense information or strategic data for the benefit of a foreign state, foreign intelligence entity, or foreign agent.
- c. Cyber Sabotage — Refers to the intentional disruption, degradation, manipulation, or destruction of computer systems, communications networks, satellites, or critical information infrastructure for the purpose of impairing national defense, national security, or essential government operations.
- d. Critical Information Infrastructure — Refers to systems, assets, or networks whose incapacity or destruction would have a debilitating impact on national security, economic security, public safety, or public health, including but not limited to:
 - i. telecommunications networks;
 - ii. satellite systems;
 - iii. military communications systems;
 - iv. government information systems;
 - v. financial and banking systems;
 - vi. energy and power grids;
 - vii. transportation networks;
 - viii. submarine communication cables.
- e. National Defense Information — Refers to classified or restricted information relating to military operations, intelligence activities, defense technology, national security strategies, or strategic infrastructure of the Republic of the Philippines.

- f. Foreign Intelligence Entity — Refers to any foreign government, military organization, intelligence service, state-owned enterprise, or organization acting on behalf of or under the direction of a foreign state.
- g. Foreign Agent — Refers to any individual who knowingly acts on behalf of a foreign intelligence entity for the purpose of conducting espionage or intelligence activities against the Republic of the Philippines.

ARTICLE III PROHIBITED ACTS

Section 4. Espionage. — Any person who knowingly obtains, copies, records, transmits, or communicates national defense information to a foreign state, foreign intelligence entity, or foreign agent, with intent or reason to believe that such information will be used to the detriment of the national security of the Republic of the Philippines, shall be guilty of espionage punishable under Section 14 of this Act.

Section 5. Cyber Espionage. — Any person who intentionally and without lawful authority commits any of the following acts for the benefit of a foreign state, foreign intelligence entity, or foreign agent shall be guilty of cyber espionage punishable under Section 15 of this Act:

- a. hacks or infiltrates government computer systems;
- b. accesses classified or sensitive national security databases;
- c. penetrates military or intelligence communications networks;
or
- d. obtains strategic data from critical information infrastructure systems.

Acts punishable under this section shall be without prejudice to liability under Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

Section 6. Hacking of Communication Infrastructure. — Any person who intentionally and without lawful authority commits any of the following acts for the benefit of a foreign state, foreign intelligence entity, or foreign agent:

- a. interferes with or infiltrates telecommunications networks;
- b. accesses, disrupts, or sabotages satellite communication systems;
- c. tampers with submarine communication cables or internet backbone infrastructure; or
- d. disrupts military command-and-control communications

systems, shall be guilty of cyber espionage or cyber sabotage, punishable under Section 15 of this Act.

Section 7. Possession of Espionage Devices. — Any person who possesses, manufactures, develops, or deploys equipment or software designed or primarily intended for espionage activities, including but not limited to:

- a. surveillance malware;
- b. signal interception devices;
- c. covert communication transmitters; or
- d. satellite interception equipment,

with intent to use such equipment or software to commit espionage shall be guilty of espionage punishable under Section 14 of this Act.

Section 8. Economic Espionage. — Any person who knowingly steals, copies, transmits, or delivers sensitive industrial, technological, or proprietary information relating to:

- a. defense industries;
- b. telecommunications technology;
- c. semiconductor technology;
- d. military equipment; or
- e. cybersecurity systems,

for the benefit of a foreign state, foreign intelligence entity, or foreign agent shall be guilty of espionage punishable under Section 14 of this Act.

Section 9. Espionage through Research Institutions. — Any person who knowingly and intentionally uses universities, research institutions, laboratories, or joint technology programs to obtain classified national defense information or strategic technology for the benefit of a foreign intelligence entity shall be guilty of espionage punishable under Section 14 of this Act.

Nothing in this section shall be interpreted to restrict legitimate academic collaboration or scientific research not involving classified or restricted national defense information.

Section 10. Espionage through Digital Platforms. — Any person who uses online platforms, encrypted communications systems, or social media networks to knowingly recruit agents, transmit classified national defense information, or coordinate espionage activities for a foreign intelligence entity shall be guilty of espionage punishable under Section 14 of this Act.

Nothing in this section shall be interpreted to restrict legitimate journalism, academic discourse, or lawful public expression that does not involve the unauthorized disclosure of classified national defense information.

Section 11. Foreign Intelligence Recruitment. — Any person who, acting on behalf of a foreign state, foreign intelligence entity, or foreign agent, knowingly recruits, solicits, induces, coerces, or attempts to recruit any Filipino citizen, government employee, member of the Armed Forces of the Philippines, researcher, contractor, or employee of critical infrastructure to obtain, disclose, transmit, or provide national defense information, strategic technology, or sensitive government data shall be guilty of espionage punishable under Section 14 of this Act.

The offense shall be deemed committed whether or not the recruitment effort succeeds or the information is actually obtained.

Section 12. Conspiracy to Commit Espionage. — When two (2) or more persons conspire to commit any offense punishable under this Act and one or more of such persons performs any overt act to effect the object of the conspiracy, each conspirator shall be liable for the offense and shall be punished in the same manner as the principal offender.

Section 13. Attempted Espionage. — Any person who attempts to commit espionage or cyber espionage under this Act by performing overt acts toward the commission of the offense, but who does not complete the act by reason of causes independent of his or her will shall suffer the penalty one degree lower than that prescribed for the consummated offense.

ARTICLE IV PENALTIES

Section 14. Espionage. — Any person who commits espionage as defined under Article III of this Act shall, upon conviction, suffer the penalty of reclusion perpetua and a fine of not less than Ten Million Pesos (₱10,000,000.00) but not more than Fifty Million Pesos (₱50,000,000.00).

Where two (2) or more acts of espionage are committed in violation of Article III of this Act, each act shall constitute a separate and distinct offense and shall be punished independently under this Act.

Section 15. Cyber Espionage. — Any person who commits cyber espionage as defined under Article III of this Act shall, upon conviction, suffer the penalty of imprisonment of twenty (20) years to reclusion perpetua and a fine of not less than Five Million Pesos

(₱5,000,000.00) but not more than Thirty Million Pesos (₱30,000,000.00).

Where two (2) or more acts of cyber espionage are committed in violation of Article III of this Act, each act shall constitute a separate and distinct offense and shall be punished independently under this Act.

Section 16. Espionage Involving Critical Infrastructure. — When the offense of espionage or cyber espionage under Article III of this Act involves telecommunications networks, military communications systems, satellite systems, submarine communication cables, or other facilities officially designated as critical infrastructure by the National Security Council or by law, the penalty of reclusion perpetua shall be imposed.

Persons convicted under this section shall not be eligible for parole under existing laws.

Section 17. Liability of Foreign Nationals. — Any foreign national who commits espionage or cyber espionage under Article III of this Act shall:

- a. upon completion of service of sentence, be deported in accordance with existing immigration laws and regulations; and
- b. be permanently barred from re—entering the Republic of the Philippines.

ARTICLE V INVESTIGATIVE POWERS

Section 18. Lead Agencies — The following agencies shall exercise investigative and enforcement authority under this Act:

- a. National Intelligence Coordinating Agency (NICA);
- b. National Bureau of Investigation (NBI);
- c. Philippine National Police (PNP);
- d. Department of Information and Communications Technology (DICT);
- e. Armed Forces of the Philippines (AFP).

These agencies shall coordinate in accordance with existing national security and intelligence frameworks subject to their respective mandates under existing laws.

Section 19. Cyber Counter-Espionage Center — The National Intelligence Coordinating Agency, in coordination with the Department of Information and Communications Technology and the Armed Forces of the Philippines, shall establish a Cyber Counter-Espionage Center to:

- a. detect cyber espionage attacks;
- b. monitor foreign cyber intelligence activities targeting Philippine systems; and
- c. protect national digital and communications infrastructure.

ARTICLE VI PROTECTION OF NATIONAL COMMUNICATION NETWORKS

Section 20. Mandatory Security Standards — Telecommunications companies and operators of critical information infrastructure operating in the Philippines shall comply with national cybersecurity and national security standards issued by the Department of Information and Communications Technology, in coordination with the National Telecommunications Commission and national security agencies.

Failure to implement adequate cybersecurity protections may result in administrative fines; suspension or revocation of operating licenses; or criminal liability when negligence results in espionage activities affecting national security.

ARTICLE VII EXTRATERRITORIAL JURISDICTION

Section 21. This Act shall apply to the following whether committed within or outside the territory of the Philippines::

- a. Filipino citizens committing acts of espionage outside Philippine territory;
- b. foreign nationals conducting espionage targeting Philippine national defense information or critical infrastructure; and
- c. cyber espionage attacks originating outside Philippine territory but directed at Philippine government systems or national security assets.

ARTICLE VIII WHISTLEBLOWER PROTECTION

Section 22. Whistleblower Protection. — Individuals who in good faith report espionage activities to competent authorities shall be protected from retaliation and may be eligible for protection under existing witness protection or government security programs.

ARTICLE IX RELATION TO EXISTING LAWS

Section 23. Relation to Existing Laws. — This Act shall supplement and, where applicable, amend the provisions of Commonwealth Act No. 616 (Espionage Act), Republic Act No. 10175 (Cybercrime Prevention Act of 2012), Republic Act No. 10844 (Department of Information and Communications Technology Act), and other relevant national security laws.

Nothing in this Act shall be construed to limit or diminish liability under other applicable laws where the acts committed constitute offenses punishable under such laws.

All laws, decrees, executive orders, rules, and regulations inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

ARTICLE X SEPARABILITY AND EFFECTIVITY

Section 24. Separability Clause — If any provision of this Act is declared unconstitutional, the remainder of the Act shall remain valid and enforceable.

Section 25. Effectivity — This Act shall take effect fifteen (15) days after publication in the Official Gazette or in a newspaper of general circulation.

Approved,