GOVERNMENT OF VIETNAM **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No. 343/2026/ND-CP	*Hanoi, September 3, 2026*

DECREE

ELABORATING ON LAW ON CYBERSECURITY WITHIN SCOPE OF MANAGEMENT OF MINISTRY OF NATIONAL DEFENSE OF VIETNAM AND ON PREVENTION OF INFORMATION CONFLICTS IN CYBERSPACE

Pursuant to the Law on Government Organization No. 63/2025/QH15;

Pursuant to the Law on National Security No. 32/2004/QH11;

Pursuant to the Law on National Defense No. 22/2018/QH14;

Pursuant to the Law on Cybersecurity No. 116/2025/QH15;

At the request of the Minister of National Defense of Vietnam;

The Government of Vietnam hereby promulgates the Decree elaborating on the Law on Cybersecurity within the scope of management of the Ministry of National Defense of Vietnam and on the prevention of information conflicts in cyberspace.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

1. This Decree elaborates on the Law on Cybersecurity, including:

a) Points a, b, c, d, dd, e, g, h, i, k, l, and m Clause 1 Article 5; Clause 2 Article 8; Clause 5 Article 9; Clause 6 Article 10; Clause 5 Article 12; Clause 5 Article 14; Clause 4 Article 25; Clause 3 Article 26; Clause 3 Article 28; Clause 3 Article 29; Clause 2 Article 30; and Clause 5 Article 34, within the scope of management of the Ministry of National Defense of Vietnam;

b) Clause 4 Article 22, regarding the prevention of information conflicts in cyberspace.

2. Matters not provided for in this Decree shall comply with the law on cybersecurity and other relevant laws.

Article 2. Regulated entities

1. This Decree applies to agencies, units, organizations, enterprises, and individuals within the scope of management of the Ministry of National Defense of Vietnam, and entities involved in the implementation of the matters specified in Point a Clause 1 Article 1 of this Decree.

2. This Decree applies to agencies, organizations, enterprises, and individuals involved in the implementation of the matters specified in Point b Clause 1 Article 1 of this Decree.

Article 3. Interpretation of terms

For the purpose of this Decree, the following terms shall be construed as follows:

Professional cybersecurity protection measures under this Decree mean the measures specified in Points e, h, i, k, and m Clause 1 Article 5 of the Law on Cybersecurity, which are applied within the scope of management of the Ministry of National Defense of Vietnam in accordance with the law.

Article 4. Principles of cybersecurity protection within scope of management of Ministry of National Defense of Vietnam and prevention of information conflicts in cyberspace

1. The Ministry of National Defense of Vietnam shall manage cybersecurity in relation to military and national defense tasks. The Ministry of Public Security of Vietnam shall, within its competence, manage cybersecurity in relation to military units engaging in civil and economic activities. For overlapping matters, the two Ministries shall agree upon regulations on cooperation.

2. The application of cybersecurity protection measures under this Decree shall be carried out within the functions, duties, and entitlements of the Ministry of National Defense of Vietnam, and in relation to military information systems and matters within the scope of management of the Ministry of National Defense of Vietnam in accordance with the law.

3. The Ministry of National Defense of Vietnam shall uniformly organize the performance of cybersecurity protection tasks and the implementation of cybersecurity protection measures for military information systems in accordance with the law on cybersecurity and other relevant laws, and shall promote the role of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam.

4. The connection, provision, and sharing of information and documents serving cybersecurity protection must satisfy requirements for the protection of state secrets and must not affect the performance of tasks within the scope of management of the Ministry of National Defense of Vietnam.

5. The assurance of data security in the military and national defense sectors must be maintained throughout the entire data lifecycle. Management and technical measures appropriate to the data classification, the level of the military information system, and the requirements of military and national defense tasks shall be applied.

6. Information conflicts in cyberspace shall be proactively prevented and blocked; cybersecurity threats shall be promptly detected and handled so as to prevent information warfare and cyber warfare in any form.

7. It is strictly prohibited to exploit or abuse cybersecurity protection measures to infringe upon the lawful rights and interests of agencies, organizations, or individuals, or to commit violations of the law. Violating organizations and individuals shall, depending on the nature and severity of their violations, be handled in accordance with the law.

Article 5. Cybersecurity protection forces and mobilization of cybersecurity protection forces within scope of management of Ministry of National Defense of Vietnam

1. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam comprise the Military Security Protection Department under the General Department of Politics of the Vietnam People's Army and the Cyberspace Operations Command.

2. Where necessary to handle a cybersecurity incident, cyberattack, or cybersecurity emergency affecting a military information system, the Ministry of National Defense of Vietnam shall take charge and cooperate with relevant agencies and organizations in mobilizing forces and means in accordance with the law.

Article 6. Training in in-depth cybersecurity knowledge and skills within scope of management of Ministry of National Defense of Vietnam

1. Standards for in-depth cybersecurity knowledge and skills, as well as the programs, contents, and certification of training in in-depth cybersecurity knowledge and skills, shall comply with the law on cybersecurity.

2. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam and agencies, units, and enterprises under the Ministry of National Defense of Vietnam that fully satisfy the conditions prescribed by the law on cybersecurity may organize training in in-depth cybersecurity knowledge and skills for entities within the scope of management of the Ministry of National Defense of Vietnam.

3. Agencies, units, and enterprises under the Ministry of National Defense of Vietnam permitted to organize training shall send information on issued training certificates to the Cyberspace Operations Command for updating and management in accordance with regulations.

4. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall develop and manage a database of trainees and instructors participating in cybersecurity training, as well as training certificates and professional certificates.

5. The Ministry of National Defense of Vietnam shall promulgate framework curricula for education and training corresponding to each standard for foundational cybersecurity knowledge and skills and each standard for in-depth cybersecurity skills, serving as the uniform basis for organizing training, assessing results, and issuing certificates; provide guidelines on training

programs and contents, standards and procedures for assessing learning outcomes, and forms of training certificates; and conduct inspections and supervision and handle violations arising from training in in-depth cybersecurity knowledge and skills within its scope of management.

Chapter II

CYBERSECURITY PROTECTION; PREVENTION AND HANDLING OF INFORMATION AND ACTS INFRINGING UPON CYBERSECURITY; ASSURANCE OF CYBER INFORMATION SECURITY AND DATA SECURITY WITHIN SCOPE OF MANAGEMENT OF MINISTRY OF NATIONAL DEFENSE OF VIETNAM

Section 1. CYBERSECURITY PROTECTION

Article 7. Classification of levels of military information systems

1. The levels of military information systems must be determined, and cybersecurity assurance solutions corresponding to such levels must be adopted.

2. The determination of levels of military information systems shall be carried out on the basis of the law on cybersecurity. The Ministry of National Defense of Vietnam shall provide guidelines on implementation with respect to military information systems within its scope of management.

3. Authority and procedures for determining levels:

a) For a military information system proposed as level 1 or level 2, the agency, unit, or enterprise directly under the Ministry of National Defense of Vietnam that is the military information system administrator shall take charge of preparing, appraising, and approving the level proposal dossier and cybersecurity assurance plan in accordance with the guidelines of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam;

b) For a military information system proposed as level 3, the agency, unit, or enterprise directly under the Ministry of National Defense of Vietnam shall prepare a level proposal dossier and cybersecurity assurance plan and submit 1 dossier to the Cyberspace Operations Command for appraisal. Within 7 working days from the date of receipt of a complete and valid dossier, the Cyberspace Operations Command shall take charge and cooperate with relevant agencies and units in appraising the level proposal dossier and cybersecurity assurance plan. Based on the appraisal results, the agency, unit, or enterprise directly under the Ministry of National Defense of Vietnam shall approve the level proposal dossier and cybersecurity assurance plan;

c) For a military information system proposed as level 4, the agency, unit, or enterprise directly under the Ministry of National Defense of Vietnam shall prepare a level proposal dossier and cybersecurity assurance plan and submit 1 dossier to the Cyberspace Operations Command for appraisal. Within 10 working days from the date of receipt of a complete and valid dossier, the Cyberspace Operations Command shall take charge and cooperate with functional agencies of the Ministry of National Defense of Vietnam in appraising the level proposal dossier and

cybersecurity assurance plan, and submit them to the Minister of National Defense of Vietnam for approval;

d) For a military information system proposed as level 5 (national security information system), the agency, unit, or enterprise directly under the Ministry of National Defense of Vietnam shall prepare a level proposal dossier and cybersecurity assurance plan and submit 1 dossier to the Cyberspace Operations Command for appraisal. Within 15 working days from the date of receipt of a complete and valid dossier, the Cyberspace Operations Command shall take charge and cooperate with relevant agencies in conducting the appraisal, report to the Minister of National Defense of Vietnam for approval of the cybersecurity assurance plan, and submit the level-5 military information system to the Prime Minister of Vietnam for approval.

4. Agencies, units, and enterprises directly under the Ministry of National Defense of Vietnam shall apply measures and fulfill cybersecurity assurance obligations corresponding to the determined levels of their military information systems.

Article 8. Military information systems included in List of national security information systems

1. The Ministry of National Defense of Vietnam shall take charge of reviewing, assessing, and preparing dossiers proposing the inclusion of military information systems in the List of national security information systems, or the removal of military information systems from the List of national security information systems when they no longer satisfy the prescribed criteria.

2. A military information system included in the List of national security information systems must satisfy the cybersecurity assurance criteria and conditions prescribed by law and shall be subject to cybersecurity protection measures appropriate to the nature and management and operational requirements of the system.

3. The Ministry of National Defense of Vietnam shall provide guidelines on the review, assessment, and preparation of proposal dossiers for military information systems.

Article 9. Cybersecurity appraisal of military information systems

1. Military information systems subject to cybersecurity appraisal:

a) Military information systems included in the List of national security information systems are mandatorily subject to cybersecurity appraisal before being put into use or when their upgrading or expansion requires changes to their design plans or cybersecurity assurance plans;

b) Military information systems other than those specified in Point a of this Clause shall be subject to cybersecurity appraisal as prescribed by the Ministry of National Defense of Vietnam.

2. Subjects of cybersecurity appraisal:

a) Design dossiers for new military information system construction investment projects;

b) Design dossiers for military information system upgrading or expansion investment projects that require changes to their design plans or cybersecurity assurance plans.

3. Contents of cybersecurity appraisal:

a) Compliance with cybersecurity regulations and conditions in the design of military information systems;

b) Conformity of protection plans, incident response and remediation plans, and arrangements of cybersecurity protection personnel.

4. The Cyberspace Operations Command shall take charge of conducting cybersecurity appraisals of military information systems.

Article 10. Procedures for cybersecurity appraisal of military information systems

1. Procedures for conducting cybersecurity appraisal:

a) After the cybersecurity level of a military information system has been appraised in accordance with the law, the military information system administrator shall submit a dossier of request for cybersecurity appraisal to the Cyberspace Operations Command;

b) The Cyberspace Operations Command shall receive and examine the dossier and issue a receipt within 3 working days from the date of receipt of a complete and valid dossier;

c) The Cyberspace Operations Command shall examine the dossier and technical documents; conduct an on-site assessment of the system; test and review security vulnerabilities; assess the cybersecurity protection, supervision, and incident response plans; and notify the cybersecurity appraisal results within 10 working days from the date of issuance of the dossier receipt.

2. A dossier of request for cybersecurity appraisal shall comprise:

a) A written request for cybersecurity appraisal;

b) Regulations, procedures, and cybersecurity assurance plans, and information on cybersecurity protection personnel; cybersecurity assurance measures for equipment, hardware, and software; technical measures for cybersecurity supervision and protection; and measures for ensuring physical security, controlling access, and preventing data leakage;

c) Documents presenting the results of the appraisal of the cybersecurity level of the military information system.

3. Where it is necessary to determine the conformity between the current condition of a military information system and the dossier of request for appraisal, the competent authority shall survey and assess the actual condition of the military information system for comparison with the dossier. Such on-site survey and assessment must not affect the normal operations of the military

information system administrator or the military information system. The period for the on-site survey and assessment shall not exceed 7 working days.

4. Cybersecurity appraisal results shall be managed in accordance with the law.

Article 11. Assessment of cybersecurity conditions of military information systems

1. Military information systems subject to assessment of cybersecurity conditions:

a) Military information systems included in the List of national security information systems are mandatorily subject to assessment of cybersecurity conditions before being put into use or when their upgrading or expansion requires changes to their design plans or cybersecurity assurance plans;

b) Military information systems other than those specified in Point a of this Clause shall be subject to assessment of cybersecurity conditions as prescribed by the Ministry of National Defense of Vietnam.

2. Contents of assessment of cybersecurity conditions:

a) Assessment of organizational and personnel conditions for ensuring cybersecurity, including the establishment of a specialized cybersecurity unit and the professional capacity of personnel;

b) Assessment of technical infrastructure conditions for ensuring cybersecurity, including security equipment systems, cybersecurity supervision systems, and data backup and recovery systems;

c) Assessment of regulations and procedures for ensuring cybersecurity;

d) Assessment of the level of compliance with cybersecurity standards and technical regulations.

3. The Cyberspace Operations Command shall take charge of assessing and certifying the eligibility for cybersecurity of military information systems, including:

a) Assessing dossiers and technical documents;

b) Conducting on-site inspection and assessment of systems;

c) Conducting trials and tests, reviewing vulnerabilities, and performing penetration assessments;

d) Simulating and conducting drills for cybersecurity scenarios, where necessary.

4. A military information system may only be put into operation and connected to networks after it has been certified as eligible for cybersecurity.

Article 12. Procedures for assessment of cybersecurity conditions of military information systems

1. Procedures for assessing cybersecurity conditions:

a) The military information system administrator shall submit a dossier of request for assessment of cybersecurity conditions to the Cyberspace Operations Command;

b) The Cyberspace Operations Command shall receive and examine the dossier, provide instructions for completing the dossier of request for assessment of cybersecurity conditions, and issue a receipt immediately upon receipt of a complete dossier;

c) The Cyberspace Operations Command shall conduct the assessment and issue a certificate of eligibility for cybersecurity within 10 working days after receiving a complete and valid dossier. If the conditions are not satisfied, within 3 working days, it shall issue a notification requiring the military information system administrator to take remedial measures and repeat the assessment procedures.

2. A dossier of request for certification of eligibility for cybersecurity of a military information system shall comprise:

a) A written request for certification of eligibility for cybersecurity;

b) The pre-feasibility study report, feasibility study report, report proposing the investment policy, and design dossier for the project on the new construction, upgrading, or expansion of the military information system prior to approval;

c) A dossier on cybersecurity assurance solutions for the military information system.

3. The Cyberspace Operations Command shall conduct the assessment in accordance with the prescribed procedures; ensure objectivity and accuracy; and maintain the confidentiality of information during the assessment. The agency or unit requesting the assessment shall cooperate in providing complete information and documents; ensure the technical conditions necessary for the assessment; and comply with the requirements of the assessing authority.

Article 13. Cybersecurity supervision of military information systems

1. Military information systems shall be subject to cybersecurity supervision appropriate to their levels, nature, scale, scope of operation, and the requirements of military and national defense tasks.

2. The Ministry of National Defense of Vietnam shall take charge of organizing cybersecurity supervision of military information systems.

3. Responsibilities of military information system administrators:

a) Organize cybersecurity supervision of information systems under their management;

b) Establish self-supervision and self-warning mechanisms and mechanisms for receiving warnings of cybersecurity threats, cybersecurity incidents, weaknesses, and security vulnerabilities;

c) Cooperate with the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam in organizing cybersecurity supervision.

4. Contents of cybersecurity supervision:

a) Monitoring and supervising the operation of military information systems, network infrastructure, information technology equipment, and related components;

b) Collecting and analyzing system log data, network traffic, and information necessary for detecting cybersecurity risks;

c) Detecting signs of cyberattacks, unauthorized intrusions, dissemination of malicious software, and acts that threaten cybersecurity;

d) Supervising cybersecurity vulnerabilities and weaknesses;

dd) Analyzing and assessing the extent of impact of cybersecurity threats and incidents;

e) Issuing warnings of cybersecurity threats.

Article 14. Procedures and authority for cybersecurity supervision of military information systems

1. Procedures for conducting cybersecurity supervision:

a) Establishing technical systems and mechanisms for cybersecurity supervision;

b) Collecting data and information serving cybersecurity supervision;

c) Analyzing and assessing collected data and information;

d) Identifying threats and the extent of impact of incidents and acts infringing upon cybersecurity;

dd) Issuing warnings of cybersecurity threats and incidents to military information system administrators;

e) Applying necessary measures to prevent, handle, and remedy cybersecurity threats and incidents in accordance with the law.

2. Responsibilities of military information system administrators:

a) Organize the implementation of cybersecurity supervision;

b) Upon detecting signs of a cyberattack or cybersecurity threat, verify the information and assess the level of threat; implement technical measures to prevent and mitigate its impact; notify relevant agencies and units for cooperation in handling; and report to the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam where an incident is serious or exceeds their handling capacity;

c) After handling a cybersecurity incident, inspect and reassess the cybersecurity condition of the system; restore the normal operation of the information system; prepare dossiers and retain information relating to the handling of the cybersecurity incident; and report the results to the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam.

3. Responsibilities of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam:

a) Take charge of organizing cybersecurity supervision of military information systems;

b) Direct and provide guidelines for military information system administrators to connect and maintain cybersecurity supervision systems and centralized malware prevention and combat systems connected to the Cyberspace Operations Command;

c) Decide on the provision of necessary technical information and data serving supervision activities in accordance with the law.

4. Information and data collected from cybersecurity supervision shall be managed and utilized in accordance with the law on cybersecurity, the law on protection of state secrets, and regulations of the Ministry of National Defense of Vietnam.

Article 15. Cybersecurity inspection of military information systems

1. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall take charge and cooperate with relevant agencies and units in conducting cybersecurity inspections of military information systems.

2. Cases of cybersecurity inspection:

a) When electronic equipment or cybersecurity services are put into use in a military information system;

b) When there is a change in the current condition of a military information system;

c) Periodically, as prescribed;

d) Upon the occurrence of a cybersecurity incident or an act infringing upon cybersecurity.

3. Subjects of cybersecurity inspection:

a) Hardware systems, software systems, and digital devices;

b) Cybersecurity protection procedures, regulations, and measures;

c) Information stored, processed, and transmitted;

d) Incident response and remediation plans;

dd) Measures for protecting state secrets and preventing data disclosure and loss;

e) Personnel dossiers.

4. Contents of cybersecurity inspection:

a) Compliance with the law on cybersecurity and the law on protection of state secrets;

b) The implementation, maintenance, and effectiveness of cybersecurity assurance plans and measures and cybersecurity incident response and remediation plans;

c) The detection and assessment of weaknesses, security vulnerabilities, and malicious software, and the testing of the susceptibility of military information systems to penetration, where necessary;

d) Other inspection contents as decided by the inspecting authority or requested by the military information system administrator.

5. Military information system administrators shall provide information and documents and comply with the requirements of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam for the purpose of cybersecurity inspections.

Article 16. Procedures for cybersecurity inspection of military information systems

1. Procedures for cybersecurity inspection:

a) Notify the cybersecurity inspection plan or decision, except in the case of an ad hoc inspection intended to promptly prevent risks of harm to national security or military security;

b) Conduct the cybersecurity inspection in cooperation with the military information system administrator and without interrupting the normal operation of the system, except where necessary to protect national security or military security;

c) Prepare minutes of the cybersecurity inspection process and results, and manage and retain such minutes in accordance with regulations;

d) Notify the cybersecurity inspection results.

2. Where it is necessary to preserve the current condition of a military information system for the investigation and handling of violations of the law, verification of a cybersecurity incident, or remediation of weaknesses or security vulnerabilities, such preservation shall be carried out at the request and under the guidance of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam.

Article 17. Response to and remediation of cybersecurity incidents affecting military information systems

1. Activities for responding to and remedying cybersecurity incidents affecting military information systems include:

a) Detecting and identifying cybersecurity incidents;

b) Preserving the scene and collecting information and evidence;

c) Containing an incident and limiting the scope of its impact;

d) Analyzing, assessing, and classifying the cybersecurity incident;

dd) Implementing incident response and remediation measures and restoring the system;

e) Verifying the cause and tracing the origin of the incident;

g) Conducting investigations and handling the incident in accordance with the law where there are signs of a crime or violation of the law.

2. Procedures for responding to and remedying cybersecurity incidents:

a) Detecting and receiving information on a cybersecurity incident: Detecting the incident through supervision systems and receiving warnings and incident reports from the military information system administrator;

b) Identifying and assessing threats: Analyzing data and signs of abnormalities to identify the incident and assess the scope and extent of its impact on the military information system;

c) Organizing incident response: Implementing technical measures to prevent and limit the spread of the incident; isolating affected system components; and removing malicious code and malicious software or eliminating unauthorized intrusions;

d) Remedying the incident and restoring the system: Remedying cybersecurity vulnerabilities and weaknesses; restoring affected data, system configurations, and services; and inspecting and assessing the system to ensure its safe operation before putting it back into operation;

dd) Reporting the cybersecurity incident, analyzing its causes, and proposing preventive measures.

3. The military information system administrator shall perform the activities specified in Clause 1 of this Article. Where an incident exceeds its handling capacity, the administrator shall notify the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam to conduct the cybersecurity incident response.

4. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall receive and verify information on incidents; provide guidance to military information system administrators on implementing incident-handling measures; and organize forces, means, and technical measures to conduct incident response.

Article 18. Use of cryptography to protect cyber information

1. Data and information classified as state secrets must be protected using state cipher when stored or transmitted in cyberspace in accordance with the laws on cipher, protection of state secrets, and data.

2. The storage and transmission of data and information in the military and national defense sectors that are not classified as state secrets shall comply with regulations of the Ministry of National Defense of Vietnam.

Article 19. Collection of electronic data in cyberspace within scope of management of Ministry of National Defense of Vietnam

1. The specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall collect electronic data for the investigation and handling of violations and crimes that undermine safety or security or infringe upon national security or military security in cyberspace.

2. Procedures for collecting electronic data to serve the investigation and handling of violations and crimes that undermine safety or security or infringe upon national security or military security in cyberspace shall comply with the law.

3. The Military Security Protection Department shall decide on the application of electronic data collection measures to serve the investigation and handling of violations and crimes that undermine safety or security or infringe upon national security or military security in cyberspace.

Article 20. Professional cybersecurity protection measures

1. The Minister of National Defense of Vietnam shall decide on the application of professional cybersecurity protection measures to serve cybersecurity protection for military information systems and the investigation, verification, and handling of cases in cyberspace within the scope of management of the Ministry of National Defense of Vietnam.

2. Within their competence, the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall take charge of and organize the implementation of professional cybersecurity protection measures.

3. Procedures for applying professional cybersecurity protection measures:

a) Detecting or receiving information or warnings, or identifying signs of threats or violations of the law on cybersecurity;

b) Organizing the assessment of threats, the extent of their impact, and their scope of effect;

c) Proposing professional cybersecurity protection measures appropriate to the nature and severity of the threat or violation;

d) Considering and deciding on the application of professional cybersecurity protection measures according to competence;

dd) Organizing the implementation of the measures decided upon;

e) Monitoring, inspecting, and assessing compliance with and implementation of the measures;

g) Consolidating and reporting task performance results in accordance with regulations.

4. Information, documents, data, and results obtained during the application of professional cybersecurity protection measures shall be managed and used in accordance with the law on protection of state secrets and regulations of the Ministry of National Defense of Vietnam.

Section 2. ASSURANCE OF DATA SECURITY

Article 21. Responsibilities for assuring data security

1. Information system administrators, data administrators, and relevant organizations and individuals shall ensure the security of data within the scope of management of the Ministry of National Defense of Vietnam and cooperate with the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam in assuring data security.

2. With respect to data processed in cyberspace within the scope of management of the Ministry of National Defense of Vietnam, the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall provide guidance to information system administrators, data administrators, and relevant organizations and individuals on applying

technical and management measures to prevent, detect, and block acts prohibited under the Law on Cybersecurity and other relevant laws.

Article 22. Contents of data security assurance within scope of management of Ministry of National Defense of Vietnam

The Ministry of National Defense of Vietnam shall take charge of organizing the assurance of data security for military information systems and data affecting military and national defense tasks in accordance with the laws on cybersecurity, data, personal data protection, protection of state secrets, and cipher, and the following provisions:

1. Implement management, technical, and professional measures to ensure the security of data within the scope of management of the Ministry of National Defense of Vietnam; classify and manage military and national defense data and apply measures for its protection.

2. Prescribe standards, technical regulations, and data security assurance requirements appropriate to military and national defense activities.

3. Supervise, inspect, and assess data security risks; detect, prevent, block, and handle acts infringing upon the data security of military information systems.

4. Protect military information systems and respond to and remedy data security incidents affecting such systems.

5. Decide on the use of cryptography to ensure information and data security for military information systems.

6. Appraise, inspect, assess, and decide on the external storage, processing, sharing, or transfer of data within its scope of management.

7. Apply internal security measures to prevent risks of data disclosure or loss.

Section 3. PREVENTION AND HANDLING OF INFORMATION AND ACTS OF USING INFORMATION TECHNOLOGY OR ELECTRONIC EQUIPMENT TO INFRINGE UPON NATIONAL SECURITY AND SOCIAL ORDER AND SAFETY IN CYBERSPACE; ASSURANCE OF CYBER INFORMATION SECURITY

Article 23. Authority and responsibilities of specialized cybersecurity protection forces under Ministry of National Defense of Vietnam

1. Take charge of processing information and preventing and combating acts of using information technology or electronic equipment to infringe upon national security and social order and safety in relation to military information systems.

2. Take charge of processing information and preventing and combating acts in cyberspace where a competent authority determines that information or acts of using information technology

or electronic equipment to infringe upon national security and social order and safety are created or committed by organizations or individuals within the scope of management of the Ministry of National Defense of Vietnam, obstruct the performance of tasks, or infringe upon the lawful rights and interests of agencies, units, enterprises, organizations, or individuals within the scope of management of the Ministry of National Defense of Vietnam.

3. Cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam in protecting national security and social order and safety in cyberspace.

4. The Military Security Protection Department may apply the measures specified in Clause 1 Article 5 of the Law on Cybersecurity to serve the prevention, investigation, and handling of information and acts infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace within the scope of management of the Ministry of National Defense of Vietnam.

5. The Cyberspace Operations Command may apply the measures specified in Clause 1 Article 5 of the Law on Cybersecurity as appropriate to cyberspace operations.

6. The application of each measure specified in Clause 1 Article 5 of the Law on Cybersecurity by the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam shall comply with the law and regulations of the Ministry of National Defense of Vietnam.

Article 24. Responsibilities of information system administrators and enterprises providing services on telecommunications networks, Internet, and value-added services in cyberspace

1. Information system administrators and domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace shall cooperate with the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam, at the request of competent authorities and in accordance with law, in cases within the scope of management of the Ministry of National Defense of Vietnam.

2. Enterprises under the Ministry of National Defense of Vietnam providing services on telecommunications networks, the Internet, and value-added services in cyberspace shall identify IP addresses and ensure cyber information security in accordance with Clauses 2 and 3 Article 25 of the Law on Cybersecurity through the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam to protect state secrets and ensure the performance of military and national defense tasks.

Article 25. Responsibilities of organizations and individuals drafting, posting, or disseminating information in cyberspace

1. Comply with requests to remove or correct information, or cease disseminating information containing content falling into cases prescribed by law within the scope of management of the Ministry of National Defense of Vietnam, and provide related information and data at the request

of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam.

The time limit for fulfilling the obligation to remove information shall not exceed 6 hours from the receipt of the request; in an emergency, the time limit shall not exceed 1 hour. The results of implementation shall also be notified as requested.

2. Proactively notify and report to the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam upon detecting information or acts in violation of the law in cyberspace relating to military or national defense matters.

3. Apply technical measures prescribed by law to prevent the continued dissemination of violating information within the scope under their management, including disabling sharing, copying, and dissemination functions; preventing the reposting of such information; and removing links and data relating to violating content at the request of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam.

4. Provide information, documents, and electronic data relating to violating content in an intact, complete, and accurate manner at the request of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam within no more than 24 hours or, in an emergency, no more than 6 hours.

Article 26. Responsibilities of administrators and operators of associations, groups, channels, pages, and accounts in cyberspace

1. Administer and operate associations, groups, channels, pages, and accounts in cyberspace in accordance with the law on cybersecurity and other relevant laws.

2. Cooperate and comply with requests of the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam in handling information and acts falling into cases prescribed by law within the scope of management of the Ministry of National Defense of Vietnam:

a) Remove violating information and provide information and data relating to associations, groups, channels, pages, and accounts under their administration;

b) Apply technical measures prescribed by law to prevent the dissemination and reposting of violating content.

3. Refrain from deleting traces, destroying data, or obstructing verification and investigation activities.

Chapter III

CYBERSECURITY PRODUCTS AND SERVICES AND TRADING IN CYBERSECURITY PRODUCTS AND SERVICES SERVING MILITARY TASKS

Article 27. Cybersecurity products and services serving military tasks

1. Cybersecurity products include:

a) Cybersecurity inspection and assessment products, comprising hardware devices and software with the following basic functions: scanning, inspecting, and analyzing the configurations, current conditions, and log data of information systems; detecting vulnerabilities and weaknesses; and providing cybersecurity risk assessments;

b) Cybersecurity supervision products, comprising hardware devices and software with the following basic functions: supervising and analyzing data stored and transmitted in information systems; collecting and analyzing log data in real time; and detecting and issuing warnings of abnormal events that pose cybersecurity risks;

c) Anti-attack and anti-intrusion products, comprising hardware devices and software with the basic function of preventing attacks against and intrusions into information systems;

d) Other cybersecurity products prescribed by the Ministry of National Defense of Vietnam.

2. Cybersecurity services include:

a) Cybersecurity inspection and assessment services, comprising services for scanning, inspecting, and analyzing the configurations, current conditions, and log data of information systems; detecting vulnerabilities and weaknesses; and providing cybersecurity risk assessments;

b) Information security services not using civil cryptography, comprising services that assist users in assuring the confidentiality of information and information systems without using civil cryptographic systems;

c) Cybersecurity consultancy services, comprising services that provide consultancy and assistance in inspecting, assessing, implementing, designing, and developing cybersecurity assurance solutions;

d) Cybersecurity supervision services, comprising services for supervising and analyzing data traffic transmitted in information systems; collecting and analyzing log data in real time; and detecting and issuing warnings of abnormal events that pose cybersecurity risks;

dd) Cybersecurity incident response services for handling and remedying incidents that threaten the cybersecurity of information systems;

e) Services for recovering deleted or damaged data in information systems;

g) Cyberattack prevention and combat services for preventing attacks against and intrusions into information systems through the supervision, collection, and analysis of events occurring in information systems;

h) Digital investigation and analysis services, comprising services for collecting, preserving, analyzing, and recovering data or electronic evidence to serve the handling of cybersecurity incidents and other activities prescribed by law;

i) Cybersecurity training and drill services, comprising education, training, and awareness-raising services and the organization of scenario-based drills to enhance cybersecurity assurance capacity;

k) Other cybersecurity services prescribed by the Ministry of National Defense of Vietnam.

Article 28. Management of trading, export, and import of cybersecurity products and services serving military tasks

1. Enterprises trading in cybersecurity products and services must possess a license for trading in cybersecurity products and services in accordance with the law on cybersecurity. Cybersecurity products and services provided to the Ministry of National Defense of Vietnam for military tasks shall be exempt from the procedures for applying for a license from the competent state management authority and are not required to be specified in the license for trading in cybersecurity products and services.

2. The Ministry of National Defense of Vietnam shall manage the cybersecurity products and services specified in this Article and shall:

a) Promulgate standards and technical regulations and manage quality;

b) Register, designate, and manage the operations of organizations certifying conformity with standards and technical regulations;

c) Manage and license the export and import of cybersecurity products;

d) Inspect and supervise the trading in cybersecurity products and services serving military tasks.

Chapter IV

PREVENTION OF INFORMATION CONFLICTS IN CYBERSPACE

Section 1. SUPERVISION, DETECTION, AND WARNING OF INFORMATION CONFLICTS IN CYBERSPACE

Article 29. Supervision, detection, and warning of information conflicts in cyberspace

1. The supervision, detection, and warning of information conflicts in cyberspace constitute part of cybersecurity supervision activities and shall be conducted regularly and continuously by specialized cybersecurity protection forces and information system administrators in accordance with the law on cybersecurity.

2. Administrators of national security information systems and international connection gateways shall cooperate with specialized cybersecurity protection forces in developing, deploying, training, and maintaining systems for supervising, detecting, and issuing warnings of information conflicts in cyberspace.

3. Supervision information shall be received, analyzed, and processed by specialized cybersecurity protection forces, and warnings shall be issued to relevant organizations and individuals.

Article 30. Receipt and handling of information conflicts in cyberspace

1. Information system administrators shall receive and handle information conflicts in cyberspace and cooperate with specialized cybersecurity protection forces in responding to incidents and preventing information conflicts in cyberspace.

2. Specialized cybersecurity protection forces shall receive, analyze, and handle information conflicts in cyberspace between domestic and foreign organizations and individuals as specified in Clause 1 Article 41 and Clause 1 Article 42 of this Decree.

3. Information conflicts in cyberspace shall be handled by specialized cybersecurity protection forces in a manner that does not escalate the conflict and prevents warfare in any form.

4. The Ministry of National Defense of Vietnam shall take charge of establishing a focal point for receiving and handling information on information conflicts in cyberspace within its scope of management and relating to national sovereignty in cyberspace, and shall cooperate with the Ministry of Public Security of Vietnam in handling cases relating to national security and social order and safety.

5. The Ministry of Public Security of Vietnam shall take charge of handling information conflicts in cyberspace relating to national security and social order and safety, and shall cooperate with the Ministry of National Defense of Vietnam in handling cases relating to national defense and national sovereignty in cyberspace.

Section 2. IDENTIFICATION OF ORIGIN OF INFORMATION IN CYBERSPACE

Article 31. Contents of identification of origin of information conflicts in cyberspace

1. Identification of the origin of an information conflict in cyberspace includes identifying data packets, information, source addresses, destination addresses, service ports, the time, methods, and tactics of the information conflict in cyberspace, and identifying the entities, purposes, and extent of the information conflict in cyberspace.

2. The identification of the origin of information conflicts in cyberspace must comply with the law on cybersecurity, the law on protection of state secrets, and other relevant laws.

Article 32. Results of identification of origin of information conflicts in cyberspace

1. The results of identifying the origin of an information conflict in cyberspace comprise documents, supporting evidence, and evidence collected by specialized cybersecurity protection forces in a manner that ensures objectivity, accuracy, and scientific validity.

2. The results of identifying the origin of an information conflict in cyberspace shall be lawfully used in combating and preventing information conflicts in cyberspace.

Article 33. Roles and responsibilities in identifying origin of information conflicts in cyberspace

1. Identification of the origin of an information conflict in cyberspace is intended to detect, collect, and assess information and use it as supporting evidence and evidence.

2. Specialized cybersecurity protection forces shall have the authority to identify the origin of information conflicts in cyberspace.

3. Administrators of information systems involved in an information conflict in cyberspace shall cooperate with specialized cybersecurity protection forces in accurately identifying the origin of the information conflict in cyberspace.

4. Agencies, organizations, and individuals shall, within the scope of their duties and entitlements, promptly and fully provide specialized cybersecurity protection forces with information, supporting evidence, and evidence serving the identification of the origin.

5. Agencies, organizations, and individuals participating in or associated with an information conflict in cyberspace shall provide accurate information and shall not provide false or misleading information. Any person who intentionally provides false or misleading information shall, depending on the severity of the violation, face criminal prosecution or administrative penalties.

Section 3. FILTERING AND BLOCKING, REMEDIATION, AND ELIMINATION OF INFORMATION CONFLICTS IN CYBERSPACE

Article 34. Filtering and blocking information in cyberspace

1. Telecommunications and Internet service providers shall filter and block information where any of the following factors exists:

a) The origin of an information conflict in cyberspace affecting national defense, national security, or national sovereignty in cyberspace has been identified;

b) The reasonableness of a request made by the party affected by the information conflict in cyberspace has been clearly established;

c) A written request or a request transmitted through a technical system serving the command and administration of specialized cybersecurity protection forces has been made.

2. The filtering and blocking of information must be conducted according to the proper competence and in relation to the proper subjects and must not affect the lawful activities of organizations and individuals.

Article 35. Remediation of information conflicts in cyberspace

1. An information system administrator shall organize the remediation of information conflicts in cyberspace within its scope of management and shall be subject to the direction of specialized cybersecurity protection forces in organizing such remediation.

2. An information system administrator shall develop plans for remedying information conflicts in cyberspace within its scope of management and consolidate and report information on the situation and results of such remediation to specialized cybersecurity protection forces.

3. Specialized cybersecurity protection forces shall cooperate with information system administrators in remedying information conflicts relating to national defense, national security, and state agencies in accordance with Clause 1 Article 41 and Clause 1 Article 42 of this Decree.

4. Measures for remedying an information conflict shall be applied when all of the following conditions are satisfied:

a) The occurrence of an information conflict has been determined;

b) The information conflict affects or poses a risk of affecting the operations of an agency, organization, or individual;

c) A request or direction has been issued by a competent authority with respect to a case relating to national defense or national security.

Article 36. Elimination of information conflicts in cyberspace

1. Specialized cybersecurity protection forces shall eliminate information conflicts in cyberspace.

2. Telecommunications and Internet service providers shall cooperate with specialized cybersecurity protection forces in eliminating information conflicts in cyberspace.

3. An information conflict in cyberspace shall be eliminated when the following factors exist:

a) The origin of the information conflict in cyberspace has been clearly identified;

b) The available human resources, technological and technical measures, and diplomatic efforts are sufficient to eliminate the information conflict in cyberspace;

c) Relevant organizations and individuals have been notified, directly or indirectly, by telephone, email, or mass media, of the source of information causing the information conflict in cyberspace.

Article 37. Cooperation in filtering and blocking, remedying, and eliminating information conflicts in cyberspace

1. The Ministry of National Defense of Vietnam shall take charge of filtering and blocking, remedying, and eliminating information conflicts in cyberspace relating to agencies, units, enterprises, individuals, or the functions and duties of the Ministry of National Defense of Vietnam, and shall cooperate with the Ministry of Public Security in cases relating to national security and social order and safety.

2. The Ministry of Public Security of Vietnam shall take charge of filtering and blocking, remedying, and eliminating information conflicts in cyberspace relating to national security and social order and safety, and shall cooperate with the Ministry of National Defense of Vietnam in cases relating to national defense.

3. The Ministry of Science and Technology of Vietnam shall cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam as specified in Clauses 1 and 2 of this Article in providing technical guidance and coordination and requiring telecommunications and Internet service providers to implement filtering and blocking, remediation, and elimination measures at the request of competent authorities.

4. The Ministry of Culture, Sports and Tourism of Vietnam shall cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam as specified in Clauses 1 and 2 of this Article in managing, filtering and blocking, remedying, and eliminating conflict-related information in the press, radio, television, and electronic information environment in accordance with the law.

5. Information system administrators shall cooperate in implementing measures for filtering and blocking, remedying, and eliminating information conflicts within their scope of management at the request of competent authorities.

6. Telecommunications and Internet service providers shall implement technical measures, provide information and data, and cooperate with competent authorities in the process of filtering and blocking, remedying, and eliminating information conflicts.

Section 4. COMMUNICATION, DISSEMINATION, EDUCATION, ORIENTATION OF PUBLIC OPINION, AND INTERNATIONAL COOPERATION IN PREVENTION OF INFORMATION CONFLICTS IN CYBERSPACE

Article 38. Communication, dissemination, education, and orientation of public opinion regarding prevention of information conflicts in cyberspace

1. Contents of communication, dissemination, education, and orientation of public opinion:

a) Policies and laws on the prevention of information conflicts in cyberspace;

b) The position, role, and importance of preventing information conflicts in cyberspace;

c) Methods, tactics, and risks of causing information conflicts in cyberspace;

d) Knowledge and skills for proactively preventing information conflicts in cyberspace;

d) Knowledge and skills for proactively preventing information conflicts in cyberspace;

e) Responsibilities of agencies, organizations, enterprises, and individuals for preventing information conflicts in cyberspace;

g) Other contents relating to the prevention of information conflicts in cyberspace.

2. Forms of communication, dissemination, education, and orientation of public opinion:

a) In-person meetings, exchanges, dialogues, and discussions;

b) Through mass media;

c) Through activities at educational and training institutions and cybersecurity associations;

d) Through legal knowledge competitions and community activities;

dd) Other forms consistent with the law.

3. Communication, dissemination, education, and orientation of public opinion shall be strengthened for administrators of national security information systems; enterprises providing network infrastructure and telecommunications and Internet services; associations and clubs operating in the fields of information technology, cybersecurity, electronics, and telecommunications; and local areas in which incidents causing information conflicts in cyberspace frequently occur.

4. The Ministry of National Defense of Vietnam and the Ministry of Public Security of Vietnam shall cooperate with the Ministry of Education and Training of Vietnam and relevant committees, ministries, and central authorities in organizing communication, dissemination, education, and orientation of public opinion regarding the prevention of information conflicts in cyberspace, in accordance with the entitlements and responsibilities specified in Clause 1 Article 41 and Clause 1 Article 42 of this Decree to improve awareness, responsibility, and effectiveness in preventing information conflicts in cyberspace.

Article 39. Contents of international cooperation in prevention of information conflicts in cyberspace

1. International cooperation in collecting, researching, and exchanging information and experience regarding the prevention of information conflicts in cyberspace; cooperating in education, advanced training, and professional training on the prevention of information conflicts

in cyberspace; organizing international conferences and seminars on matters relating to the prevention of information conflicts in cyberspace; and providing physical, technical, and technological support to strengthen specialized cybersecurity protection forces.

2. International cooperation to eliminate risks of information conflicts in cyberspace originating from the territory of one country and targeting another country, and cooperation in investigations upon receipt of international requests to prevent information conflicts in cyberspace, must comply with the law on cybersecurity, the law on national defense, and international treaties to which the Socialist Republic of Vietnam is a contracting party.

3. Consultation with other countries regarding activities for preventing information conflicts in cyberspace and cooperation in resolving matters relating to the prevention of information conflicts in cyberspace.

Article 40. Refusal of international cooperation in prevention of information conflicts in cyberspace

Specialized cybersecurity protection forces and relevant Vietnamese agencies and organizations may refuse requests for cooperation whose contents are detrimental to sovereignty, national defense, national security, or the interests of the State, or are inconsistent with Vietnamese law or international treaties to which the Socialist Republic of Vietnam is a contracting party.

Section 5. RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS, INDIVIDUALS, AND TELECOMMUNICATIONS AND INTERNET SERVICE PROVIDERS FOR PREVENTING INFORMATION CONFLICTS IN CYBERSPACE

Article 41. Ministry of National Defense of Vietnam

1. The Ministry of National Defense of Vietnam shall assume responsibility before the Government of Vietnam for taking charge and cooperating with relevant agencies in preventing information conflicts in cyberspace for the following purposes:

a) Preventing and combating information warfare and cyber warfare;

b) Preventing foreign military forces or domestic or foreign organizations from using technological and information-technical measures to cause damage to information or military information systems.

2. Take charge of preventing information conflicts in cyberspace to protect national sovereignty in cyberspace in accordance with its functions and duties.

3. Organize the development of professional forces with high combat readiness and coordinate and utilize national defense resources to prevent information conflicts in cyberspace for the purposes specified in Clause 1 of this Article.

4. Draft, amend, or supplement and submit to competent authorities for promulgation, or promulgate according to its competence, documents concerning the prevention of information conflicts in cyberspace.

5. Take charge and cooperate with relevant agencies in organizing education and advanced training for human resources performing tasks of preventing information conflicts in cyberspace.

6. Direct its subordinate forces to take charge and cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam in organizing professional training and drills on the prevention of information conflicts in cyberspace.

7. Invest in and provide equipment and means for performing tasks of preventing information conflicts in cyberspace.

8. Exchange information with the Ministry of Public Security of Vietnam, the Ministry of Foreign Affairs of Vietnam, and relevant committees, ministries, and central authorities regarding the prevention of information conflicts in cyberspace.

9. Conduct international cooperation in the prevention of information conflicts in cyberspace.

Article 42. Ministry of Public Security of Vietnam

1. The Ministry of Public Security of Vietnam shall assume responsibility before the Government of Vietnam for taking charge and cooperating with relevant agencies in preventing information conflicts in cyberspace between two or more domestic or foreign organizations using technological and information-technical measures to cause damage to national security or social order and safety, in accordance with the functions and duties of the Ministry of Public Security of Vietnam.

2. Take charge of preventing information conflicts in cyberspace to protect national security and social order and safety and to prevent and combat crime.

3. Take charge and cooperate with the Ministry of National Defense of Vietnam and relevant agencies and organizations in developing and implementing measures to detect, prevent, combat, and eliminate activities in cyberspace that threaten national security or social order and safety, and to prevent and combat crime; handle acts infringing upon national sovereignty in cyberspace in accordance with its assigned functions and duties, the law on cybersecurity, and its scope of management.

4. Direct its subordinate forces to take charge and cooperate with the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam in organizing professional training and drills on the prevention of information conflicts in cyberspace, protection of national security and social order and safety, and prevention and combat of crime; and conduct international cooperation in the prevention of information conflicts in cyberspace.

5. Regularly exchange and provide the Ministry of National Defense of Vietnam with information on the situation, risks to information security, and activities relating to the prevention of information conflicts in cyberspace.

Article 43. Ministry of Foreign Affairs of Vietnam

The Ministry of Foreign Affairs of Vietnam shall take charge and cooperate with the Ministry of National Defense of Vietnam and the Ministry of Public Security of Vietnam in implementing solutions for protecting information systems of overseas representative missions of the Socialist Republic of Vietnam, and shall cooperate in conducting foreign affairs relating to activities for preventing information conflicts in cyberspace.

Article 44. Ministry of Science and Technology of Vietnam

1. Advise the Government of Vietnam on identifying scientific and technological tasks relating to activities for preventing information conflicts in cyberspace.

2. Direct agencies and units under its management to cooperate with the specialized cybersecurity protection forces under the Ministry of National Defense of Vietnam and the Ministry of Public Security of Vietnam in performing scientific and technological tasks and developing scientific and technological capacity for protecting national security information systems.

Article 45. Ministry of Finance of Vietnam

Based on proposals of ministries and central authorities, the Ministry of Finance of Vietnam shall take charge of submitting to competent authorities the allocation of funding in annual state budget estimates of committees, ministries, and central authorities for activities of preventing information conflicts in cyberspace in accordance with the law on the state budget.

Article 46. Committees, ministries, central authorities, and People's Committees of provinces and centrally affiliated cities

1. Assign agencies advising on the state management of information technology and cybersecurity to perform tasks of preventing information conflicts in cyberspace, including supervising, detecting, issuing warnings, identifying origins, and remedying information conflicts in cyberspace.

2. Take charge and cooperate with specialized cybersecurity protection forces in implementing plans for protecting information systems within their scope of management; remain ready to mobilize forces and means to participate in activities for preventing information conflicts in cyberspace in accordance with the law.

3. Cooperate with specialized cybersecurity protection forces in implementing and urging the implementation of policies, strategies, and plans for preventing information conflicts in

cyberspace; and handle and remedy incidents relating to information conflicts in cyberspace within their scope of management.

Article 47. Organizations and individuals

1. Information system administrators shall implement measures to protect information systems under their management and prevent information conflicts in cyberspace affecting such systems, and shall closely cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam in implementing measures to prevent information conflicts in cyberspace.

2. Agencies, organizations, and individuals shall prevent acts that pose risks of information conflicts in cyberspace originating from their information systems and cooperate in identifying the origin of and remedying the consequences of information conflicts in cyberspace.

Article 48. Telecommunications and Internet service providers

1. Fully provide information and cooperate in identifying and blocking sources of information causing conflicts in cyberspace at the request of specialized cybersecurity protection forces.

2. Implement cybersecurity assurance solutions; organize supervision and detection; and promptly notify specialized cybersecurity protection forces of sources of information causing conflicts in cyberspace.

3. Cooperate with the Ministry of National Defense of Vietnam and the Ministry of Public Security of Vietnam in implementing technological and information-technical solutions and measures to prevent information conflicts in cyberspace.

Chapter V

IMPLEMENTATION PROVISIONS

Article 49. Entry into force and transitional provisions

1. This Decree comes into force as of September 3, 2026. Decree No. 142/2016/ND-CP dated December 1, 2016 of the Government of Vietnam shall cease to have effect from the effective date of this Decree.

2. Military information systems whose levels have already been determined shall retain their determined levels from the effective date of this Decree. Within 12 months from the effective date of this Decree, such systems must satisfy the cybersecurity protection conditions, standards, and measures corresponding to their levels as prescribed by the Ministry of National Defense of Vietnam.

Article 50. Implementation

1. The Minister of National Defense of Vietnam shall urge, inspect, and provide guidance on the implementation of this Decree.

2. Ministers, Directors of ministerial agencies, and Presidents of People's Committees of provinces and centrally affiliated cities shall implement this Decree.

ON BEHALF OF THE GOVERNMENT
PP. PRIME MINISTER
DEPUTY PRIME MINISTER

Phan Van Giang

---

*This translation is made by **THƯ VIỆN PHÁP LUẬT**, Ho Chi Minh City, Vietnam and for reference purposes only. Its copyright is owned by **THƯ VIỆN PHÁP LUẬT** and protected under Clause 2, Article 14 of the Law on Intellectual Property.Your comments are always welcomed*