THE NATIONAL ASSEMBLY	SOCIALIST REPUBLIC OF VIETNAM
--------	Independence - Freedom - Happiness

Law No. 24/2018/QH14	*Hanoi, June 12, 2018*

CYBERSECURITY LAW

Pursuant to the Constitution of Socialist Republic of Vietnam;

The National Assembly promulgates the Cybersecurity Law.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

This Law provides for protection of national security and public order in cyberspace; responsibility of relevant organizations and individuals.

Article 2. Definitions

For the purpose of this document, the terms below are construed as follows:

1. *"cybersecurity"* means assurance that activities in cyberspace do not harm national security, public order, the lawful rights and interests of any organization or individual.

2. *"cybersecurity protection"* includes prevention, discovery, and actions against violations of cybersecurity.

3. *"cyberspace"* means a network of information technology (IT) infrastructure which includes telecommunications network, the Internet, computer network, communication systems, information processing and control systems, databases; cyberspace is where people's activities are not limited by space and time.

4. *"national cyberspace"* means a cyberspace established, managed and controlled by the Government.

5. *"national cyberspace infrastructure"* means a system of infrastructure serving creation, transmission, collection, processing, storage and exchange of in the national cyberspace, including:

a) Transmission system, which includes the national transmission system, international transmission system, satellite system, transmission systems of telecommunications service

providers (TSP), Internet service providers (ISP) and providers of value-added services in cyberspace (VAS);

b) Core service systems, including national information channeling and routing system, domain name system (DNS), public key infrastructure/certificate authority (PKI/CA) and Internet connection services by TSPs, ISPs and VAS providers;

c) Services and IT applications including online services, interconnected IT applications serving administration by major business and finance organizations; national database.

Online services including electronic government, electronic commerce, websites, online forums, social networks and blogs;

d) IT infrastructure of smart cities, the Internet of things (IoT), mixed reality systems, cloud computing, big data, rapid data and artificial intelligence.

6. *"international internet gateway"* means the place through which network data is transmitted between Vietnam and other countries.

7. *"cybercrime"* means a crime that involves the use of cyberspace, information technology or electronic devices as defined in Criminal Code.

8. *"cyberattack" means the use of cyberspace, information technology or electronic devices to sabotage or interrupt the telecommunications network, the Internet, computer network, communication systems, information processing and control systems, databases or electronic devices.*

9. *"cyberterrorism" means an act of terrorism or financing of terrorism which involves the use of cyberspace, information technology or electronic devices.*

10. *"cyber espionage" means bypassing of warnings, firewalls, use of another person's administration or otherwise illegally acquiring information or information resources on a telecommunications network, the Internet, computer network or information processing system of an organization or individual.*

11. *"digital account"* means information used for verification and classification of right to use of applications and services in cyberspace.

12. *"cybersecurity threat" means any threat in cyberspace to national security, public order, the lawful rights and interests of an organization or individual.*

13. *"cybersecurity incident" means* an unexpected event in cyberspace that threatens *national security, public order or the lawful rights and interests of an organization or individual.*

14. *"cybersecurity* emergency*" means an event in cyberspace that* seriously *violates national security, public order or the lawful rights and interests of an organization or individual.*

Article 3. State policies on cybersecurity

1. Give priority to assurance of cybersecurity in national defense and security, socio-economic development, science and technology development and diplomacy

2. Develop health cyberspace without jeopardizing national security, public order or the lawful rights and interests of any organization or individual

3. Prioritize resources for development of a professional cybersecurity force; improve capacity of the cybersecurity force and any organization or individual that participate in cybersecurity protection; prioritize investment in research and development of cybersecurity technology.

4. Encourage and enable other organizations and individuals to participate in cybersecurity protection, handle cybersecurity threats; research and develop cybersecurity protection technologies, products, services and applications; cooperate with competent authorities in cybersecurity protection.

5. Increase international cooperation in cybersecurity.

Article 4. Cybersecurity protection principles

1. The Constitution and law must be upheld; interests of the State, the lawful rights and interests of organizations and individuals must be protected.

2. Cybersecurity protection will be carried out under leadership of Vietnam's Communist Party and management of the State; the entire political system and the people will be mobilized to ensure cybersecurity; emphasize the role of professional cybersecurity forces.

3. Combine cybersecurity protection and protection of national security information system with socio-economic development, protection of human rights and citizenship rights, enable organizations and individuals to operate in cyberspace.

4. Prevent, discover and take actions against the use of cyberspace for the purpose of violating national security, disrupting public order or violating lawful rights and interests of other organizations and individuals; eliminate cybersecurity threats.

5. Ensure cybersecurity of national cyberspace infrastructure; implement various measures to protect national security information systems.

6. National security information systems shall undergo cybersecurity appraisal and certification before being put into operation; undergo regular cybersecurity inspection and supervision in order to respond to and remediate any cybersecurity incident that occurs.

7. Application violations against regulations of law on cybersecurity shall be promptly and strictly dealt with.

Article 5. Cybersecurity protection measures

1. Cybersecurity protection measures include:

a) Cybersecurity appraisal;

b) Cybersecurity assessment;

c) Cybersecurity inspection;

d) Cybersecurity monitoring;

dd) Cybersecurity incident response and remediation;

e) Cybersecurity protection activities;

g) Use of cryptography for cybersecurity protection;

h) Request for suspension or termination of network information; termination and suspension of establishment, provision and use of telecommunications network, the Internet, production and use of radio transmitters and receivers as prescribed by law;

i) Request for removal of illegal or false information in cyberspace which violates national security, disrupts public order or violates lawful rights and interests of other organizations or individuals.

k) Collection of electronic data relevant to violation of national security, disruption of public order or violation of lawful rights and interests of any organization or individual in cyberspace;

l) Block or restrict activities of certain information system; termination, suspension or request for termination of certain information system; revocation of domain names;

m) Initiation of charges, investigation, prosecution and hearing in accordance with the Criminal Procedure Code;

n) Other measures defined by regulations of law on national security and handling administrative violations.

2. The Government shall specify procedures for application of cybersecurity protection measures, except for those mentioned in Point m and Point n Clause 1 of this Article.

Article 6. Protection of national cyberspace

The State shall implement various measures to protect the national cyberspace; take precautionary and “cybersecurity breach” means an unexpected event in cyberspace that

threatens national security, public order or the lawful rights and interests of an organization or individual.

Article 7. International cooperation in cybersecurity

1. International cooperation in cybersecurity is based on maintenance of the parties' independence and territorial integrity, non-intervention in the internal affairs of the parties, equality and mutual benefits.

2. Contents of international cooperation in cybersecurity:

a) Research and analysis of cybersecurity trends;

b) Establish a mechanism and policies for increasing cooperation between Vietnamese entities and foreign and international cybersecurity organizations;

c) Share information and experience; provide assistance in terms of cybersecurity training, equipment and technology;

d) Prevent and combat cybercrimes and cybersecurity violations; eliminate cybersecurity threats.

dd) Provide cybersecurity-related consultancy and training and develop human resources for cybersecurity;

e) Hold cybersecurity-related conventions and international forums;

g) Enter into and implement cybersecurity-related international treaties and agreements;

h) Execute programs and projects for international cooperation in cybersecurity;

i) Seek international cooperation in other cybersecurity-related activities.

3. The Ministry of Public Security is responsible to the Government for international cooperation in cybersecurity, except for international cooperation carried out by the Ministry of National Defense.

The Ministry of National Defense is responsible to the Government for international cooperation in cybersecurity within its scope.

The Ministry of Foreign Affairs shall cooperate with the Ministry of National Defense and the Ministry of Public Security in international cooperation in cybersecurity.

The Government shall decide international cooperation in cybersecurity that is relevant to more than one ministry.

4. The Ministry of Public Security is responsible to the Government for international cooperation in cybersecurity, except for international cooperation carried out by the Ministry of National Defense.

Article 8. Prohibited acts

1. Use of cyberspace for the following purposes:

a) Conducting the acts mentioned in Clause 1 Article 18 of this Law;

b) Organizing or participating in opposition to Socialist Republic of Vietnam; colluding with other people, persuading, buying off, duping, enticing or training people to oppose the government of Socialist Republic of Vietnam;

c) Distortion of history, denial of revolutionary achievements, undermining national solidarity, blasphemy, discrimination by gender or race;

d) Provision of false information for the purpose of causing public confusion or economic loss, obstructing regulatory bodies or law enforcers, violating lawful rights and interests of other organizations and individuals.

dd) Prostitution, vice, human trafficking; posting pornographic or criminal information; damaging Vietnam's good traditions, social ethics or public health;

e) Enticing, persuading or tempting others to commits crimes.

2. Any act of cyberattack, cyber terrorism, cyber espionage and cyber crimes; causing breakdown, attacking, infiltrating, overriding, interfering with, disrupting, paralyzing or sabotaging national security information systems.

3. Manufacturing or using tools, equipment, software programs or committing any act that is meant to disrupt a telecommunications network, the Internets, computer network, information systems, information processing systems and electronic control system; spreading malware in a telecommunications network, the Internets, computer network, information systems, information processing and control system; infiltrating a telecommunications network, the Internets, computer network, information systems, information processing system or electronic device control system of another person.

4. Resisting or obstructing the cybersecurity force; attacking or illegally neutralizing cybersecurity measures.

5. Taking advantage of cybersecurity protection activities to violate national security, national interests or sovereignty, disrupt public order, violate lawful rights and interests of another organization or individual or for profiteering purposes.

6. Other acts that violate this Law.

Article 9. Actions against violations against regulations of law on cybersecurity

The person who commits any of the violations mentioned in this Law will be liable to disciplinary penalties, administrative penalties or criminal prosecution depending on the nature and severity of the violation, and pay compensation for any damage caused.

Chapter II

CYBERSECURITY OF NATIONAL SECURITY INFORMATION SYSTEMS

Article 10. National security information systems

1. A national security information system is an information system which will cause serious cybersecurity issues if is broken down, infiltrated, overridden, interfered with, disrupted, paralyzed, attacked or sabotaged.

2. National security information systems include:

a) Military, security, diplomacy and cryptography information systems;

b) Systems for archiving and processing state-secret information;

c) Information systems serving storage of particularly important items and documents;

d) Information systems serving storage of materials or substances that are particularly harmful to humans or the environment;

dd) Information systems serving storage, manufacturing and management of other facilities relevant to national security;

e) Important information systems serving operation of central organizations;

g) National information systems serving energy, finance, banking, telecommunications, transport, resources and environment, chemical, health, culture and press authorities;

h) Automatic monitoring and control systems at important works relevant to national security or national security targets.

3. The Prime Minister shall promulgate and revise the list of national security information systems.

4. The Government shall provide for cooperation between the Ministry of Public Security, the Ministry of National Defense, the Ministry of Information and Communications, Vietnam Government Certificate Authority (VGCA) and other ministries in appraisal, assessment, inspection, supervision of national security information systems and responses to incidents occurring thereto.

Article 11. Appraisal of cybersecurity of national security information systems

1. Cybersecurity security means assessment of cybersecurity contents as the basis for deciding development or upgrade of the information system.

2. Cybersecurity appraisal shall be carried out for:

a) Pre-feasibility study report and design documents of the information system;

b) Information system upgrade scheme.

3. Cybersecurity appraisal contents:

a) Conformity of the design with cybersecurity regulations and conditions;

b) Conformity with the cybersecurity protection and incident response plan, cybersecurity personnel.

4. The power to appraise cybersecurity of national security information systems:

a) The professional cybersecurity force of the Ministry of Public Security shall appraise cybersecurity of national security information systems, except for those mentioned in Point b and Point c of this Clause;

b) The professional cybersecurity force of the Ministry of National Defense shall appraise cybersecurity of military information systems;

c) VGCA shall appraise cybersecurity of information systems thereof.

Article 12. Assessment of cybersecurity of national security information systems

1. Assessment of cybersecurity means considering the cybersecurity capacity of the information system before such system is put into operation.

2. A national security information system shall have:

a) Regulations, procedures and plans for assurance of cybersecurity; system operators and administrators;

b) Assurance of cybersecurity of equipment, hardware and software that are system components;

c) Technical measures for monitoring and protecting cybersecurity; measures for protecting the automatic monitoring and control system. the Internet of things (IoT), mixed reality systems, cloud computing, big data, rapid data and artificial intelligence systems;

d) Physical protection measures, including isolation, prevention of data leak, information transmission control.

3. The power to assess cybersecurity of national security information systems:

a) The professional cybersecurity force of the Ministry of Public Security shall assess and certify cybersecurity of national security information systems, except for those mentioned in Point b and Point c of this Clause;

b) The professional cybersecurity force of the Ministry of National Defense shall assess and certify cybersecurity of military information systems;

c) VGCA shall assess and certify cybersecurity of information systems thereof.

4. A national security information systems will be put into operation after its cybersecurity is certified.

5. The Government shall elaborate Clause 2 of this Article.

Article 13. Inspection of cybersecurity of national security information systems

1. Inspection of cybersecurity means determination of cybersecurity status of an information system, information system infrastructure or information stored, processed or transmitted within the information system in order to prevent, discover and handle cybersecurity threats; implement plans and measures for ensuring normal operation of the information system.

2. A national security information system shall undergo cybersecurity inspection in the following cases:

a) An or network information security service or electronic device is put into use in the information system;

b) There are changes to status of the information system;

c) Annual inspection;

d) Ad hoc inspection in case of cybersecurity incidents or cybersecurity violations; at the request of a cybersecurity authority; expiration of the deadline for remediating vulnerabilities recommended by a professional cybersecurity force.

3. Cybersecurity inspection shall be carried out for:

a) Hardware systems, software systems, digital devices in information systems;

b) Cybersecurity regulations and measures;

c) Information stored, processed and transmitted within the information system;

d) Cybersecurity incident response and remediation plans of the information system admin;

dd) Measures for protection of state secrets; prevention of leak of state secrets through technical channels;

e) Cybersecurity protection.

4. The administrator of a national security information system shall carry out cybersecurity inspection in the cases mentioned in Point a through c Clause 2 of this Article and send the annual inspection report to the professional cybersecurity force of the Ministry of Public Security (or the Ministry of National Defense for military information systems) before October.

5. Ad hoc inspection of cybersecurity:

a) The cybersecurity force shall send a written notification to the system's administrator at least 12 hours before the inspection in case of a cybersecurity incident or cybersecurity violation; at least 72 hours if the inspection is meant to serve state management of cybersecurity or the deadline for remediation of vulnerabilities has expired;

b) Within 30 days from the end of the inspection, the cybersecurity force shall send a notification and requests to the administrator in case weaknesses or vulnerabilities are found; provide instructions if requested by the admin;

c) The cybersecurity force of the Ministry of Public Security shall carry out ad hoc inspection of national security information systems other than those under the management of the Ministry of National Defense, cryptography systems of VGCA and cryptography products provided by VGCA for protection of state-secret information.

The professional cybersecurity force of the Ministry of National Defense shall carry out ad hoc cybersecurity inspection of military information systems.

VGCA shall carry out ad hoc cybersecurity inspection of its cryptography systems and cryptography products it provides for protection of state-secret information.

d) Administrators of national security information systems shall cooperate with professional cybersecurity forces in the ad hoc cybersecurity inspections.

6. The cybersecurity inspection results shall be kept confidential as prescribed by law.

Article 14. Supervision of cybersecurity of national security information systems

1. Cybersecurity supervision means collection and analysis of information in order to identify cybersecurity threats, cybersecurity incidents, weaknesses and vulnerabilities, malicious codes and hardware, based on which warnings and solutions will be made.

2. d) Administrators of national security information systems shall cooperate with professional cybersecurity forces in supervision of the systems; establish a mechanism to give warnings and receive warnings about cybersecurity threats, cybersecurity incidents, vulnerabilities, malicious codes, malicious hardware and develop emergency response plans.

3. Professional cybersecurity forces shall supervise national security information systems under their management; give warnings and cooperate with their administrators in responding to cybersecurity threats, cybersecurity incidents, vulnerabilities, malicious codes and malicious hardware.

Article 15. Response and remediation of cybersecurity incidents occurring to National security information systems

1. Response and remediation of cybersecurity incidents occurring to National security information systems include the following activities:

a) Discovery and identification of cybersecurity incidents;

b) Scene protection and evidence collection;

c) Limiting the scope of and damage caused by the incident;

d) Determination of the scope of response and subjects that need assistance;

dd) Verification, analysis, assessment and classification of the cybersecurity incident;

e) Execution of the response and remediation plan;

g) Identifying causes and origins of the incident;

h) Investigation and handling;

2. Administrators of national security information systems shall devise plans for responding to and remediating cybersecurity incidents that occur to their systems; implement such plans in case a cybersecurity incident occurs and promptly inform the competent cybersecurity force.

3. Coordinating response and remediation of cybersecurity incidents occurring to national security information systems:

a) Professional cybersecurity forces of the Ministry of Public Security shall coordinate response and remediation of cybersecurity incidents that occur to national security information systems other than those mentioned in Point b and Point c of this Clause; participate in cybersecurity incident response and remediation activities on request; inform the system administrators whenever a cyberattack or cybersecurity incident is discovered;

b) The professional cybersecurity force of the Ministry of National Defense shall coordinate response and remediation of cybersecurity incidents that occur to military information systems;

c) VGCA shall coordinate response and remediation of cybersecurity incidents that occur to their cryptography systems.

4. Other organizations and individuals are responsible for participating in response and remediation of cybersecurity incidents that occur to national security information systems at the request of the coordinating authority.

Chapter III

PREVENTION AND ACTIONS AGAINST CYBERSECURITY VIOLATIONS

Article 16. Prevention and handling of cyberinformation that is meant to oppose the government of Socialist Republic of Vietnam, cause riots, disturb the peace, humiliate or slander, or violate economic management laws

1. A piece of information in cyberspace will be considered propaganda against the government of Socialist Republic of Vietnam if it:

a) slanders or defames the people's government;

b) is used for psychological warfare; provokes war of aggression; causes discrimination against or hostility towards a race, religion or country;

c) offends the people or desecrate the national flag, national anthem, political leaders, honored people or national heroes.

2. A piece of information in cyberspace will be considered provoking riots or disturbing the peace if it:

a) persuades, encourages, deceives, threatens people or causes discrimination for the purpose of armed activities or use of violent force to oppose the people's government.

b) encourages, deceives, threatens or persuades people to participate in public gathering intended to cause disruption or oppose law enforcers or obstructs operation of an organization, thus threatens public order and security.

3. A piece of information in cyberspace will be considered humiliating or slandering if it:

a) seriously harms another person’s dignity or honor;

b) is fabricated to harm another person’s dignity or honor or violate lawful rights and interests of another organization or individual.

4. Information in cyberspace that is meant to commit violations against regulations of law on economic management includes:

a) Fabricated or false information about products, goods, money, bonds, treasury bills, checks and other financial instruments;

b) Fabricated or false information about finance, banking, e-commerce, electronic payment, foreign exchange, capital raising, multi-level marketing, securities.

5. Other fabricated or false information in cyberspace that is meant to cause public confusion or economic loss, obstructing regulatory bodies or law enforcers, violate lawful rights and interests of other organizations and individuals.

6. Administrators of information systems have the responsibility to implement administrative and technical measures for prevention, discovery, intervention and removal of the information mentioned in Clause 1 through 5 of this Article on their systems at the request of professional cybersecurity forces.

7. Professional cybersecurity forces and competent authorities shall apply the measures mentioned in Point h, i and l Clause 1 Article 5 of this Article to handle the cyberinformation mentioned in Clause 1 through 5 of this Article.

8. TSPs, ISPs, VAS providers and information system administrators shall cooperate with competent authorities in handling the information mentioned in Clause 1 through 5 of this Article.

9. Any organization or individual that devises, posts or spreads the information mentioned in Clause 1 through 5 of this Article shall remove it at the request of the professional cybersecurity force and bear legal responsibility.

Article 17. Prevention and response to cyber espionage; protection of state-secret information, business secrets, family secrets and privacy in cyberspace

1. The following acts are considered cyber espionage or deliberate violation of state-secret information, work secrets, business secrets, family secrets and privacy in cyberspace:

a) Illegal obtainment, trade, collection, deliberate revelation of information classified as state secret information, work secrets, business secrets, family secrets and privacy which harm the dignity, reputation or lawful rights and interests of another organization or individual;

b) Deliberate deletion, causing damage, loss or changes to information classified as state-secret information, work secrets, business secrets, family secrets and privacy that is transmitted or stored in cyberspace;

c) Deliberately changing, canceling or neutralizing a technical measure that is meant to protect state-secret information, work secrets, business secrets, family secrets or privacy;

d) Posting state-secret information, work secrets, business secrets, family secrets and privacy in cyberspace against the law;

dd) Illegally eavesdropping or recording conversations;

e) Other acts that are considered deliberate violation of state-secret information, work secrets, business secrets, family secrets or privacy in cyberspace:

2. Information system administrators have the responsibility to:

a) Carry out cybersecurity inspection to detect and remove malicious codes and hardware, fix weaknesses and vulnerabilities; discover and prevent infiltration or other risks to cybersecurity;

b) Implement administrative and technical measures to prevent, discover and stop cyber espionage, infringement upon e state-secret information, work secrets, business secrets, family secrets or infringement upon privacy in their systems and remove relevant information;

c) Comply with requests of cybersecurity forces regarding prevention and response to cyber espionage and protection of state-secret information, work secrets, business secrets, family secrets and privacy in their systems.

3. The agencies responsible for drafting and storing state-secret information and documents are also responsible for protection of such information and documents which are stored in computers, other devices or transmitted in cyberspace in accordance with regulations of law on protection of state secrets.

4. The Ministry of Public Security, except for the cases mentioned in Clause 5 and Clause 6 of this Article, has the responsibility to:

a) Carry out inspection of cybersecurity of national security information systems to detect and remove malicious codes and hardware, fix weaknesses and vulnerabilities; discover and prevent network infiltration;

b) Carry out inspection of cybersecurity of communication equipment, products and services, digital and electronic devices before they are used in any national security information systems;

c) Carry out supervision of cybersecurity of national security information systems to detect and stop illegal collection of state-secret information;

d) Discover and take actions against acts of posting, storing or exchanging information and documents classified as state secrets in cyberspace;

dd) Participate in research and manufacturing of products serving storage and transmission of state-secret information and documents, and cryptographic products;

e) Inspect the protection of state secrets in cyberspace by state authorities and administrators of national security information systems;

g) Provide training in protection of state secrets in cyberspace, prevention and response to cyberattack, and cybersecurity protection for the cybersecurity forces as prescribed in Clause 2 Article 30 of this Law.

5. The Ministry of National Defense has the responsibility mentioned in Point a through e Clause 4 of this Article regarding military information systems.

6. VGCA is responsible for organizing implementation of regulations of law on cryptography in order to protect state-secret information stored and transmitted in cyberspace.

Article 18. Prevention and response to use of cyberspace, information technology or electronic devices for violations of regulations of law on national security and public order

1. Use of cyberspace, information technology or electronic devices for violations of regulations of law on national security and public order includes:

a) Posting or spreading the information mentioned in Clause 1 through 5 of Article 16 in cyberspace and the acts mentioned in Clause 1 Article 17 of this Law;

b) Appropriation of property; online gambling or organization thereof; theft of service involving voice over Internet protocol (VoIP); intellectual property and copyright infringement in cyberspace;

c) Making fake websites of other organizations and individuals; forging, stealing, illegally using, trading, collecting or exchanging others' credit information or bank accounts; illegally issuing, providing or using payment facilities;

d) Advertising or trading in banned goods/services;

dd) Instructing others to commit violations of law;

e) Other uses of cyberspace, information technology or electronic devices for violations of regulations of law on national security and public order.

2. Professional cybersecurity forces have the responsibility to prevent and respond to use of cyberspace, information technology or electronic devices for violations of regulations of law on national security and public order.

Article 19. Prevention and response to cyberattacks

1. Acts of cyberattacks and relevant acts include:

a) Spread of software programs that are harmful to a telecommunications network, the Internet, computer network, communication system, information processing and control systems, databases or electronic devices;

b) Obstructing, causing disruption, paralysis or interruption of data transmission of a telecommunications network, the Internet, computer network, communication system, information processing system or electronic device control system;

c) Infiltrating, causing damage or illegally obtaining data stored or transmitted through a telecommunications network, the Internet, computer network, communication system, information processing and control systems, databases or electronic devices;

d) Infiltrating, creating or exploiting weaknesses or vulnerabilities of a system to illegally obtain information for profiteering;

d) Producing, trading, exchanging, giving tools, equipment, software programs that are meant to attack a telecommunications network, the Internet, computer network, a communication system, information processing and control systems, database or electronic devices;

e) Other acts affecting normal operation of a telecommunications network, the Internet, computer network, communication system, information processing and control systems, database or electronic devices;

2. Administrators of information systems have the responsibility to implement technical measures for preventing the acts mentioned in Point a, b, c, d, e Clause 1 of this Article from affecting their systems.

3. In case of a cyberattack that violates or threatens to violate national security, national interests, sovereignty or disrupt public order, the professional cybersecurity force shall take charge and cooperate with the system administrator, relevant organizations and individuals in tracing the origin of the attack, collecting evidence; request TSPs, ISPs and VAS providers to filter information serving the attack and provide relevant information and documents.

4. Responsibility for prevention and response to cyberattack:

a) The Ministry of Public Security shall take charge and cooperate with relevant ministries in prevention, detection and response to the acts mentioned in Clause 1 of this Article if they violate or threaten to violate national security, national interest, sovereignty or seriously disrupt public order nationwide, except of the cases mentioned in Point b and Point c of this Clause;

b) The Ministry of National Defense shall take charge and cooperate with relevant ministries in prevention, detection and response to the acts mentioned in Clause 1 of this Article if they are committed against military information systems;

c) VGCA shall take charge and cooperate with relevant ministries in prevention, detection and response to the acts mentioned in Clause 1 of this Article if they are committed against cryptography systems under its management.

Article 20. Prevention and response to cyberterrorism

1. Competent authorities shall implement the measures against cyberterrorism provided for in this Law, Article 29 of the Law on Cyberinformation security and regulations of law against cyberterrorism.

2. Information system administrators shall regularly review and inspect their systems to eliminate the risks of cyberterrorism

3. Any sign of cyberterrorism must be promptly reported to cybersecurity forces. The authority that receives the information about cyberterrorism shall promptly notify a professional cybersecurity force.

4. The Ministry of Public Security shall take charge and cooperate with relevant ministries in prevention and response to cyberterrorism, neutralize the sources of cyberterrorism, take actions against cyberterrorism and minimize damage to information systems, except for the cases mentioned in Clause 5 and Clause 6 of this Article.

5. The Ministry of National Defense shall take charge and cooperate with relevant ministries in prevention and response to cyberterrorism against military information system.

6. VGCA shall take charge and cooperate with relevant ministries in prevention and response to cyberterrorism against cryptography systems under its management.

Article 21. Prevention and response to cybersecurity emergencies

1. Cybersecurity emergencies include:

a) Provoking information in cyberspace that might lead to riots, disruption of public order or terrorism;

b) Attack on a national security information system;

c) Large-scale and intense attacks on multiple information systems;

d) Cyberattack meant to destroy a national security work or target;

dd) Cyber attack that seriously violates national security, national interest, sovereignty, social order or the lawful rights and interests of an organization or individual.

2. Responsibility for prevention and response to cybersecurity emergencies:

a) Professional cybersecurity forces shall cooperate with administrators of national security information systems in implementing specific measures for prevention, detection and response to cybersecurity emergencies;

b) Telecommunication enterprises, Internet enterprises, IT enterprises, TSPs, ISPs, VAS providers, relevant organizations and individuals shall cooperate with professional cybersecurity forces of the Ministry of Public Security in prevention, detection and response to cybersecurity emergencies.

3. Actions to be taken in response to a cybersecurity emergency:

a) Promptly implement the cybersecurity emergency prevention and response plan; avoid, eliminate or minimize damage caused by the cybersecurity emergency;

b) Inform relevant organizations and individuals;

c) Collect relevant information; continuously monitor the cybersecurity emergency;

d) Analyze information; estimate damage and impacts caused by the cybersecurity emergency;

dd) Stop providing cyberinformation within a certain area or disconnect from the international internet gateway;

e) Provide forces and equipment for prevention and elimination of the cybersecurity emergency:

g) Other measures specified in the Law on National security.

4. Responsibility to respond to cybersecurity emergencies:

a) The organization or individual that detects a cybersecurity emergency must promptly inform a professional cybersecurity force and implement the measures mentioned in Point a and Point b Clause 3 of this Article;

b) The Prime Minister shall make decisions or authorize the Minister of Public Security to make decisions regarding cybersecurity emergencies that occur nationwide or locally or to a specific target.

The Prime Minister shall make decisions or authorize the Minister of National Defense to make decisions regarding cybersecurity emergencies that occur to cryptography of VGCA;

c) Professional cybersecurity forces shall take charge and cooperate with relevant organizations and individuals in implementing the measures mentioned in Clause 3 of this Article to respond to cybersecurity emergencies;

d) Relevant organizations and individuals shall cooperate with professional cybersecurity forces in implementing measures for prevention and response to cybersecurity emergencies.

Article 22. Cybersecurity protection activities

1. Cybersecurity protection activities are organized by professional cybersecurity forces to protect national security and public order.

2. Cybersecurity protection activities include:

a) Monitoring status of national security;

b) Prevent and respond to attacks; protect national security information systems;

c) Paralyze or limit activities using cyberspace to violate national security or public order;

d) Launch cyberattacks to protect national security and public order.

3. The Ministry of Public Security shall take charge and cooperate with relevant ministries in cybersecurity protection activities.

Chapter IV

CYBERSECURITY PROTECTION ACTIVITIES

Article 23. Cybersecurity protection in central and local authorities and political organizations

1. Struggle for cybersecurity protection includes:

a) Develop and complete regulations on use of local networks and the Internet; plans for assurance of cybersecurity of information systems; plans for cybersecurity incident response and remediation;

b) Implement and apply various cybersecurity protection plans, measures, technologies to information systems, information and documents created, stored and transmitted within information systems under their management;

c) Provide refresher training in cybersecurity for officials, public employees and other employees; improve the capacity of cybersecurity forces;

d) Ensure cybersecurity during provision of public services in cyberspace, exchange of information with other entities; internal and external transmission of information and other activities specified by the Government;

dd) Invest in and develop infrastructure suitable for assurance of cybersecurity of information systems;

e) Inspect cybersecurity of information systems; prevent and deal with violations against regulations of law on cybersecurity; respond to and remediate cybersecurity incidents.

2. Heads of organizations are responsible for organizing cybersecurity protection activities under their management.

Article 24. Inspection of cybersecurity of information systems other than national security information systems

1. An information system other than national security information systems shall undergo cybersecurity inspection in the following cases:

a) There is a violation of regulations of law on cybersecurity that violates national security or seriously disrupts public order;

b) The inspection is requested by the administrator of the information system.

2. Subjects of cybersecurity inspection:

a) Hardware systems, software systems, digital devices in information systems;

b) Information stored, processed and transmitted within the information system;

c) Measures for protection of state secrets; prevention and response to leak of state secrets through technical channels.

3. Administrators of information systems shall inform the professional cybersecurity force of the Ministry of Public Security upon discovery of cybersecurity breach on their systems.

4. The professional cybersecurity force of the Ministry of Public Security shall carryout cybersecurity inspection of information systems in the cases mentioned in Clause 1 of this Article.

5. The cybersecurity force shall inform the information system administrator in writing at least 12 hours before the inspection.

Within 30 days from the end of the inspection, the cybersecurity force shall send a notification and requests to the administrator in case weaknesses or vulnerabilities are found; provide instructions if requested by the admin.

6. The cybersecurity inspection results shall be kept confidential as prescribed by law.

7. The Government shall elaborate procedures for cybersecurity inspection mentioned in this Article.

Article 25. Protection of cybersecurity of national cyberspace infrastructure and international internet gateways

1. Protection of cybersecurity of national cyberspace infrastructure and international internet gateways shall combine cybersecurity protection and socio-economic development; international internet gateways located within Vietnam's territory will be given priority; investments in national cyberspace infrastructure will be given priority.

2. Responsibility of users of national cyberspace infrastructure and international internet gateways:

a) Protect cybersecurity under their management; facilitate administration and inspection and comply with cybersecurity requirements by competent authorities;

b) Enable and implement administrative and technical measures necessary for competent authorities to protect cybersecurity upon request.

Article 26. Assurance of information security in cyberspace

1. Information mentioned in Clause 1 through 5 Article 16 of this Law and other information that violates national security are not allowed on websites, web portals and social media pages of any organization or individual.

2. Domestic and overseas providers of telecommunications services, internet services and value-added services in Vietnam’s cyberspace have the responsibility to:

a) Verify users’ information when they open digital accounts; protect confidentiality of users’ information and accounts; provide users’ information for professional cybersecurity forces of the Ministry of Public Security upon request in writing to serve investigation into cybersecurity violations;

b) Block and delete information mentioned in Clause 1 through 5 Article 16 of this Law on their services or information systems within 24 hours after a request is given by the cybersecurity force of the Ministry of Public Security or a competent authority of the Ministry of Information and Communications; keep a log of such events to serve investigation into cybersecurity violations for a certain period of time specified by the Government;

c) Stop providing or refuse to provide the aforementioned services for the organizations or individuals that post the information mentioned in Clause 1 through 5 Article 16 of this Law upon request by the cybersecurity force of the Ministry of Public Security or a competent authority of the Ministry of Information and Communications.

3. Domestic and overseas providers of telecommunications services, internet services and value-added services in Vietnam’s cyberspace that collect, analyze or process private information or data about relationships of their service users or data created by their service users in Vietnam shall retain such data for a specific period of time defined by the Government.

Overseas enterprises mentioned in this Clause shall open branches or representative offices in Vietnam.

4. The Government shall elaborate Clause 3 of this Article.

Article 27. Cybersecurity research and development

1. Cybersecurity research and development include:

a) Development of cybersecurity software and equipment;

b) Solutions for appraisal of cybersecurity software and equipment; remediation of weaknesses, vulnerability and malicious software;

c) Methods for inspection of functionality of hardware and software;

d) Methods for state-secret information, work secrets, business secrets, personal secrets, family secrets and privacy; security of information transmitted in cyberspace;

dd) Tracing origins of information transmitted in cyberspace;

e) Elimination of cybersecurity threats;

g) Development of cyberspace boot camps and cybersecurity testing environment;

h) Technical initiatives for improving cybersecurity skills and awareness;

i) Cybersecurity forecasting;

k) Cybersecurity practice research and cybersecurity theory development.

2. All organizations and individuals have the right to carry out cybersecurity research and development.

Article 28. Improvement of cybersecurity independence

1. The State will encourage and enable all organizations and individuals to improve their capacity of cybersecurity and the ability to product, inspect, assess digital devices, network services and network applications.

2. The Government shall implement the following measures to improve cybersecurity independence:

a) Promote transfer, research, mastery and development of cybersecurity technology, products, services and applications;

b) Promote application of new and advanced cybersecurity technologies;

c) Organize provision of training, development and employment of cybersecurity personnel

d) Enhance business environment, improve competitiveness and support for enterprises that research or produce cybersecurity products services and applications.

Article 29. Protection of children in cyberspace

1. Children have the right to be protected, access information, participate in social activities and entertainment, personal information confidentiality and other rights in cyberspace.

2. Administrators of information systems, TSPs, ISPs and VAS providers have the responsibility to make sure information on their systems or services are not harmful children and do not violate children's rights; block and delete information harmful to children or violating children's rights; Promptly inform and cooperate with the cybersecurity force of the Ministry of Public Security whenever such information is detected.

3. Organizations and individuals operating in cyberspace shall cooperate with competent authorities I protecting children's rights in cyberspace and prevent information harmful to children in accordance with this Law and children laws.

4. Organizations, parents, teachers, caretakers and relevant individuals have the responsibility to protect children's rights and protect children in cyberspace in accordance with children laws.

5. Professional cybersecurity forces and other competent authorities shall implement every measure necessary for preventing, detecting, intervening harms to children or violations of children's rights by means of cyberspace.

Chapter V

ASSURANCE OF CYBERSECURITY PROTECTION

Article 30. Cybersecurity forces

Cybersecurity forces include:

1. Professional cybersecurity forces of the Ministry of Public Security and the Ministry of National Defense.

2. Cybersecurity forces of other Ministries, agencies, the People's Committees of provinces and organizations managing national security information systems.

3. Other organizations and individuals mobilized to participate in cybersecurity protection.

Article 31. Assurance of human resources for cybersecurity protection

1. Vietnamese citizens having knowledge about cybersecurity, cyberinformation security or information technology are the primary resource for cybersecurity protection.

2. The State will have programs and plans for development of human resources for cybersecurity protection.

3. In case of a cybersecurity emergency, cyberterrorism, cyberattack, cybersecurity incident or cybersecurity threat, cybersecurity personnel will be mobilized by competent authorities.

Power, responsibility and procedures for mobilizing cybersecurity personnel are specified in the law on National security, the Law on National defense, the Law on the People's police and relevant laws.

Article 32. Recruitment, training and development of cybersecurity forces

1. Vietnamese citizens that are qualified in terms of moral character, health, cybersecurity, cyberinformation security or information technology knowledge may apply to cybersecurity forces.

2. Priority will be given to training and development of high-quality cybersecurity personnel.

3. Priority will be given to development of cybersecurity training centers that meet international standards; encourage and facilitate cooperation in cybersecurity between the public sector and private sector, between domestic and foreign entities.

Article 33. Cybersecurity training

1. Cybersecurity training shall be included in national defense and security education in schools and other national defense and security programs according to the Law on national defense and training education.

2. The Ministry of Public Security shall take charge and cooperate with relevant ministries in provision of cybersecurity training for cybersecurity forces, officials and public employees and other employees who participate in cybersecurity protection.

The Ministry of National Defense and VGCA shall organize provision of cybersecurity training for certain people under their management.

Article 34. Dissemination of cybersecurity knowledge

1. The State will introduce policies on nationwide dissemination of cybersecurity; encourage state agencies to cooperate with private organizations and other individuals in running cybersecurity training programs.

2. All Ministries, state agencies and organizations have the responsibility to disseminate cybersecurity knowledge among their employees.

3. The People's Committees of provinces have the responsibility to disseminate cybersecurity knowledge among local organizations and individuals.

Article 35. Cybersecurity protection funding

1. Funding for cybersecurity protection in state agencies and political organizations will be provided by state budget and included in annual the State budget estimates. Management and use of state funding shall comply with regulations of law on state budget.

2. Organizations other than those mentioned in Clause 1 of this Article shall allocate their own budget for cybersecurity protection of their information systems.

Chapter VI

RESPONSIBILITIES OF VARIOUS ORGANIZATIONS AND INDIVIDUALS

Article 36. Responsibilities of the Ministry of Public Security

The Ministry of Public Security is responsible to the Government for state management of cybersecurity and has the following responsibilities, except for the responsibilities of the Ministry of National Defense and VGCA:

1. Promulgate or request a competent authority to promulgate and provide guidelines for implementation of legislative documents on cybersecurity;

2. Develop and propose cybersecurity protection strategies, policies and plans;

3. Prevent and take actions against use of cyberspace for the purpose of violating sovereignty, national interests or national security or disrupting public order; take actions against cybercrime;

4. Ensure cyberinformation security; establish mechanisms for verifying account info; issue warnings; share information about cybersecurity and cybersecurity threats;

5. Advise the Government and the Prime Minister assigning cybersecurity tasks and cooperating in implementation of measures for cybersecurity protection, prevention and response to cybersecurity violations if they involve more than one ministry;

6. Organize cyberattack drills and cybersecurity response drill regarding national security information system;

7. Carry out inspections; settle complaints, denunciations and take actions against violations against regulations of law on cybersecurity.

Article 37. Responsibilities of the Ministry of National Defense

The Ministry of National Defense is responsible to the Government for state management of cybersecurity within its competence and has the following responsibilities:

1. Promulgate or request a competent authority to promulgate and provide guidelines for implementation of legislative documents on cybersecurity within its competence;

2. Develop and propose cybersecurity protection strategies, policies and plans within its competence;

3. Prevent and take actions against use of cyberspace for the purpose of violating national security within its competence;

4. Cooperate with the Ministry of Public Security in organizing cyberattack drills and cybersecurity response drill regarding national security information systems;

5. Carry out inspections; settle complaints, denunciations and take actions against violations against regulations of law on cybersecurity within its competence.

Article 38. Responsibilities of the Ministry of Information and Communications

1. Cooperate with the Ministry of Public Security and the Ministry of National Defense in cybersecurity protection.

2. Cooperate with relevant agencies in spreading propaganda against information that opposes the government of Socialist Republic of Vietnam mentioned in Clause 1 Article 16 of this Article.

3. Request TSPs, ISPs, VAS providers and information system administrators to remove information that violates cybersecurity laws on their systems or services.

Article 39. Responsibilities of VGCA

1. Propose cryptography-related programs, plans and legislative documents serving cybersecurity within its competence to the Ministry of National Defense or a competent authority for promulgation and organization of implementation.

2. Ensure cybersecurity of its cryptography systems and products in accordance with this Law.

3. Uniform management of cryptographic technology research; production, use and supply of cryptographic products to protect state-secret information stored and exchanged in cyberspace.

Article 40. Responsibilities of other ministries and the People's Committees of provinces

Within their competence, other ministries and the People's Committees of provinces shall ensure cybersecurity of information and information systems under their management; cooperate with the Ministry of Public Security in state management of cybersecurity.

Article 41. Responsibilities of service providers in cyberspace

1. Service providers in cyberspace have the responsibility to:

a) Issue warnings about risks to cybersecurity when using their services in cyberspace and provide instructions on risk minimization;

b) Develop plans for quick response to cybersecurity incidents; eliminating weaknesses, vulnerabilities, malicious codes, network infiltration and other security risks; deploy the response plan in case of a cybersecurity incident an inform the professional cybersecurity force specified in this law;

a) Implement technical measures and other measures for ensuring security during information collection to avoid leak or loss of data; Make a response plan in case of leak or loss of data or risk thereof, inform the incident to users and the professional cybersecurity force as prescribed by this Law;

d) Cooperate with and enable professional cybersecurity forces to protect cybersecurity.

2. TSPs, ISPs and VAS providers in Vietnam shall implement Clause 1 of this Article, Clause 2 and Clause 3 Article 26 of this Law.

Article 42. Responsibilities of cyberspace users

1. Comply with regulations of law on cybersecurity.

2. Promptly provide information about cybersecurity, cybersecurity threats and cybersecurity violations for competent authorities and cybersecurity forces.

3. Comply with cybersecurity-related requests and instructions of competent authorities; enable responsible for organizations and persons to implement cybersecurity protection measures.

Chapter VII

IMPLEMENTATION CLAUSES

Article 43. Effect

1. This Law comes into force from January 01, 2019.

2. Within 12 months from the effective date of this Law, administrators of information systems that are already on the list of national security information systems shall ensure fulfillment of all cybersecurity requirements, which will be assessed by professional cybersecurity forces in accordance with Article 12 of this Law; The Prime Minister will consider extending this deadline for up to 12 more months where necessary.

3. Within 12 months from the day on which an information system is added to the list of national security information systems, its administrator shall ensure fulfillment of all cybersecurity requirements, which will be assessed by professional cybersecurity forces in accordance with Article 12 of this Law; The Prime Minister will consider extending this deadline for up to 12 more months if necessary.

This Law is passed by the 14th National Assembly of Socialist Republic of Vietnam on June 12, 2018 during its fifth session.

PRESIDENT OF THE NATIONAL ASSEMBLY

Nguyen Thi Kim Ngan
