LAW 24
ON
CYBERSECURITY

Dated 12 June 2018

CONTENTS

GOVERNMENT

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

No.: 24/2018/QH14

Ha Noi, 12 June 2018

LAW
ON
CYBERSECURITY

Pursuant to the Constitution of the Socialist Republic of Vietnam;

The National Assembly hereby promulgates the *Law on Cybersecurity*.

CHAPTER 1

General Provisions

Article 1 *Governing scope*

This Law regulates activities of protecting national security and ensuring social order and safety in cyberspace; and the responsibilities of agencies, organizations and individuals involved.

Article 2 *Definitions*

In this Law, the following terms are construed as follows:

1. *Cybersecurity* means the assurance that activities in cyberspace will not cause harm to [infringe][1] national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals.

2. *Cybersecurity protection* means the prevention, detection, avoidance of and dealing with acts which infringe cybersecurity.

3. *Cyberspace* means the connected network of information technology [IT] infrastructure comprising telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases, where [being the environment in which] people perform social acts without being limited by space and time.

4. *National cyberspace* means cyberspace established, managed and controlled by the Government.

5. *National cyberspace infrastructure* means the system of technical and material facilities in order to [which] create, transmit, collect, process, archive and exchange information in national cyberspace comprising:

(a) Transmission systems comprising the national transmission system, internationally connected transmission systems, satellite systems and transmission systems of enterprises providing services on telecom networks and on the Internet and other added value services in cyberspace;

(b) Core service systems comprising the national information flow and navigation system, the national domain name resolution system (DNS), the national authentication system [public key infrastructure

[1] Allens footnote: Square brackets contain translator's comments only.

system] (PKI/CA), service supply systems for Internet connection and access of service providers on telecom networks, the Internet and [providers of] other added value services in cyberspace;

(c) IT services and applications comprising online services; and IT applications with network connection serving management and operation by agencies, organizations and important financial and economic groups; and the national database.

Online services comprise e-government, e-commerce, websites, online forums, social networking and blogs;

(d) IT infrastructure of smart cities[2], the internet of things, complex virtual reality systems, cloud computing, large data systems, fast data systems and artificial intelligence systems.

6. *International network gateway* means the place where transmission and reception of network signals takes place between Vietnam and other countries and territories.

7. *Cybercrime* means activities of using cyberspace, IT or e-facilities to commit a crime as regulated [defined] in the *Criminal Code*.

8. *Cyberattack* means an act of using cyberspace, IT or e-facilities to destroy [hack] and/or interrupt the operation of telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases or e-facilities of agencies, organizations and individuals.

9. *Cyberterrorism* means using cyberspace, IT or e-facilities to commit an act of terrorism or terrorist financing.

10. *Cyberespionage* means a deliberate act of bypassing a warning, access code, other code or firewall or using the administration right of another person or other means to unlawfully appropriate or collect information or information resources on a telecom network, the Internet, a computer network, an information system, an information processing and control system, a database or e-facility of an agency, organization or individual.

11. *Digital account* means information used to authenticate, verify and/or delegate power to use applications and services in cyberspace.

12. *Cybersecurity threat* means a situation occurring in cyberspace which presents indications of a threat to infringe national security, and/or to cause serious harm to social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

13. *Cybersecurity incident* [or breakdown] means any unusual occurrence in cyberspace which infringes upon national security, social order and safety and/or the lawful rights and interests of organizations and individuals.

14. *Dangerous cybersecurity situation* means an occurrence in cyberspace when there is an act which seriously infringes national security [or] causes particularly serious harm to social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

Article 3 *State policies on cybersecurity*

1. Prioritizing cybersecurity protection in national defence and security, socio-economic development, science and technology, and foreign relations.

2. Building a healthy cyberspace which does not cause harm to national security, social order and safety or to the lawful rights and interests of agencies, organizations and individuals.

---

[2] Allens footnote: The literal translation is "smart urban areas".

3. Prioritizing resources to build a specialized force responsible for the protection of cybersecurity [*Cybersecurity Task Force or CTF*][3], and upgrading the capacity of such force and of other organizations and individuals participating in the protection of cybersecurity; and prioritizing investment in research and development of science and technology for purposes of protecting cybersecurity.

4. Encouraging and facilitating organizations and individuals to participate in protecting cybersecurity and to deal with cybersecurity threats; encouraging and facilitating research and development of technology, products, services and applications for the purpose of protecting cybersecurity; and encouraging and facilitating coordination with functional agencies to protect cybersecurity.

5. Enhancing international cooperation on cybersecurity.

Article 4 *Principles of cybersecurity protection*

1. Compliance with the Constitution and law; ensuring the interests of the State and the lawful rights and interests of agencies, organizations and individuals.

2. Leadership by the Vietnamese Communist Party and uniform administration by the State; mobilization of the combined strength of the political system and the entire nation; and development of the key role of the Cybersecurity Task Force.

3. Close association between tasks for protecting cybersecurity and information systems critical for national security with the tasks for socio-economic development, ensuring human rights and civil rights, and facilitating [all] agencies, organizations and individuals to conduct activities in cyberspace.

4. Proactive prevention, detection, ending, fighting and defeating all acts using cyberspace to infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals; and readiness to prevent any cybersecurity threat.

5. Implementing cybersecurity protective activities for the national cyberspace infrastructure; applying measures to protect information systems critical for national security.

6. Information systems critical for national security shall be evaluated and certified as satisfying cybersecurity conditions prior to their commissioning for operation and use, and shall be regularly inspected [audited] and supervised for cybersecurity during the process of their use, with prompt response to and remedying of any cybersecurity incident.

7. Any act in breach of the law on cybersecurity must be promptly and strictly dealt with.

Article 5 *Measures for cybersecurity protection*

1. The measures for protecting cybersecurity comprise:

(a) Evaluation of cybersecurity;

(b) Assessment of cybersecurity conditions;

(c) Inspections [audits] of cybersecurity;

(d) Supervision of cybersecurity;

(dd) Response to and remedying any cybersecurity incident;

(e) Fighting [working hard] to protect cybersecurity;

---

[3] Allens footnote: The literal translation is "specialized protective force" but for ease of reference Cybersecurity Task Force or CTF is used throughout.

(g) Using cryptography to protect network information;

(h) Stopping, requiring the suspension of or ceasing provision of network information; suspending or temporarily suspending acts being the establishment, supply and use of telecom networks, of the Internet or being the manufacture and use of radio transmitters and receivers in accordance with law;

(i) Requiring the deletion, access to or removal of unlawful or false information in cyberspace which infringes national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals;

(k) Collecting e-data relevant to acts in cyberspace infringing national security, social order and safety or the lawful rights and interests of agencies, organizations and individuals;

(l) Freezing or restricting the operation of information systems; suspending, temporarily suspending or requiring the cessation of operation of information systems or withdrawing domain names in accordance with law;

(m) Laying charges and conducting investigations, prosecutions and trials in accordance with the Criminal Procedure Code;

(n) Other measures stipulated in the law on national security and the law on dealing with administrative offences.

2. The Government shall regulate the sequence and procedures for applying measures to protect cybersecurity, except for those prescribed in sub-clauses (m) and (n) of clause 1 above.

Article 6 *Protection of national cyberspace*

The State applies measures to protect national cyberspace; and to prevent and deal with acts infringing national security, social order and safety, and the lawful rights and interests of organizations and individuals in cyberspace

Article 7 *International cooperation on cybersecurity*

1. International cooperation on cybersecurity is conducted on the basis of respect for independence, sovereignty and territorial integrity, of non-interference in each other's internal affairs, equality and mutual benefit.

2. The contents of international cooperation on cybersecurity comprise:

(a) Research and analysis of the orientation of cybersecurity;

(b) Formulation of regimes and policies which promote cooperation regarding cybersecurity activities between Vietnamese organizations and individuals on the one hand with foreign and international organizations on the other hand;

(c) Sharing of information and experience; and assistance with training, equipment and technology which protects cybersecurity;

(d) Preventing and combating cybercrime, and acts infringing cybersecurity; and preventing cybersecurity threats;

(dd) Consultancy, training and development of cybersecurity [protective] human resources;

(e) Arranging international seminars, conferences and forums on cybersecurity;

(g) Acceding to and implementing international treaties and agreements on cybersecurity;

(h) Implementing programs and projects on international cooperation on cybersecurity;

(i) Undertaking other activities of international cooperation on cybersecurity.

3. The Ministry of Public Security is responsible before the Government to preside over coordination in conducting international cooperation on cybersecurity, except for those activities of international cooperation under the authority of the Ministry of National Defence.

The Ministry of National Defence is responsible before the Government to conduct international cooperation on cybersecurity within the managerial scope of such ministry.

The Ministry of Foreign Affairs is responsible to coordinate with the Ministry of Public Security and the Ministry of National Defence in conducting international cooperation on cybersecurity.

The Government shall make a decision in a case where international cooperation on cybersecurity falls within the responsibility of a number of ministries and branches [line ministries].

4. Any other Ministry, line ministry or locality [wishing to] undertake activities of international cooperation on cybersecurity must first obtain a written opinion from the Ministry of Public Security prior to undertaking same, except in the case of activities conducted by the Ministry of National Defence.

Article 8 *Conduct which is strictly prohibited*

1. Using cyberspace to conduct any of the following acts:

(a) The acts prescribed in article 18.1 of this Law;

(b) Organizing, activating, colluding, instigating, bribing, cheating or tricking, manipulating, training or drilling people to oppose the State of the Socialist Republic of Vietnam;

(c) Distorting history, denying revolutionary achievements, destroying the national solidarity block, conducting offences against religion, gender discrimination or racist acts;

(d) Providing false information, causing confusion amongst the Citizens, causing harm to socio-economic activities, causing difficulties for the operation of State agencies or of people performing public duties, or infringing the lawful rights and interests of other agencies, organizations and individuals;

(dd) Activities being prostitution, social evils or human trafficking; publishing information which is lewd, depraved or criminal; or destroying the fine traditions and customs of the people, social ethics or health of the community;

(e) Inciting, enticing or activating other people to commit crime.

2. Conducting a cyberattack, cyberterrorism, cyberespionage or cybercrime; causing a cybersecurity incident; attacking, infringing, or hijacking operational control of, or distorting, interrupting, stalling, paralyzing or destroying an information system critical for national security.

3. Producing or putting into use tools, facilities, software or committing an act obstructing or disrupting the operation of a telecom network, the Internet, computer network, information system, information processing and control system or e-facility; distributing an informatics program which harms the operation of a telecom network, the Internet, computer network, information system, information processing and control system, database or e-facility; or illegally accessing a telecom network, the Internet, computer network, information system, information processing and control system, database or e-facility of another person.

4. Opposing or obstructing the activities of a Cybersecurity Task Force; illegally attacking, neutralizing, disabling or rendering ineffective any cybersecurity protective measures.

5. Abusing or misusing cybersecurity protective activities in order to violate national sovereignty, interests or security, social order and safety or the lawful rights and interests of agencies, organizations and individuals, or for personal profit.

6. Other conduct in breach of this Law.

Article 9 *Dealing with breaches of the law on cybersecurity*

Any person who breaches the provisions of this Law shall, depending on the nature and seriousness of the breach, be disciplined, be subject to a penalty for an administrative offence, or be criminally prosecuted, and an offender causing loss and damage must pay compensation in accordance with law.

CHAPTER 2

Protection of Cybersecurity of Information Systems Critical for National Security

Article 10 *Information systems critical for national security*

1. *An information system critical for national security* means an information system which, if subject to an incident [breakdown], infiltration, hijacking of operational control, distortion, interruption, stoppage, paralysis, attack or destruction will seriously compromise network security [cybersecurity].

2. Information systems critical for national security comprise:

(a) Military, security, diplomatic and cipher information systems;

(b) Information systems which store and process information classified as State secret;

(c) Information systems serving the storing and preservation of objects and data of particular importance;

(d) Information systems serving preservation of materials and substances particularly dangerous to humans and the ecological environment;

(dd) Information systems serving preservation, manufacture and management of particularly important material/physical facilities relevant to national security;

(e) Important [critical] information systems serving the operation of central [State] agencies and organizations;

(g) National information systems in the sectors of energy, finance, banking, telecommunications, transport, natural resources and environment, chemicals, medical health, culture and the press;

(h) Automatic control and monitoring/surveillance systems in important construction works [or buildings] relevant to national security [or] targets critical for national security.

3. The Prime Minister of the Government shall issue, amend and supplement a list of information systems critical for national security.

4. The Government shall regulate coordination between the Ministry of Public Security, the Ministry of National Defence, the Ministry of Information and Communications, the Government Cipher Committee and other functional Ministries and line ministries in evaluation, appraisal, inspection, supervision, response and remedying incidents [breakdowns] of information systems critical for national security.

Article 11 *Evaluation of cybersecurity of information systems critical for national security*

1. *Evaluation of cybersecurity* means the activity of reviewing and assessing cybersecurity contents/items in order to provide the basis for a decision on constructing or upgrading an information system.

2. Items subject to an evaluation of cybersecurity of an information system critical for national security comprise:

(a) The pre-feasibility study report and design file for construction/building of the works of an investment project for construction of an information system prior to their approval;

(b) The plan on upgrading an information system prior to its approval.

3. Items to be evaluated regarding cybersecurity of an information system critical for national security comprise:

(a) Compliance with regulations and conditions for cybersecurity set out in the design;

(b) Conformity with plans on protection, response to and remedying any incident and on deployment of human resources protecting cybersecurity.

4. Authority to evaluate cybersecurity of an information system critical for national security is regulated as follows:

(a) The Cybersecurity Task Force [CTF] under the Ministry of Public Security shall evaluate cybersecurity of information systems critical for national security, except in the cases prescribed in sub-clauses (b) and (c) below;

(b) The CTF under the Ministry of National Defence shall evaluate cybersecurity of military information systems;

(c) The Government Cipher Committee shall evaluate cybersecurity of cipher information systems under the Government Cipher Committee.

Article 12 *Assessment of cybersecurity conditions of information systems critical for national security*

1. *Assessment of cybersecurity conditions* means reviewing whether an information system satisfies cybersecurity conditions prior to its being commissioned for operation and use.

2. Information systems critical for national security must satisfy the following conditions regarding:

(a) Regulations, procedures and plans on ensuring cybersecurity; personnel operating and administering the system;

(b) Ensuring cybersecurity of equipment, hardware and software being system components;

(c) Technical measures for supervising and protecting cybersecurity; protective measures for the automatic control and monitoring system, and for the internet of things, complex virtual reality system, cloud computing, large data system, fast data system and artificial intelligence system;

(d) Measures ensuring physical security comprising special isolation, data leakage prevention, prevention of information collection, and access control.

3. Authority to assess cybersecurity conditions of an information system critical for national security is regulated as follows:

(a) The CTF under the Ministry of Public Security shall assess and certify satisfaction of cybersecurity conditions of information systems critical for national security, except in the cases prescribed in sub-clauses (b) and (c) below;

(b) The CTF under the Ministry of National Defence shall assess and certify satisfaction of cybersecurity conditions of military information systems;

(c) The Government Cipher Committee shall assess and certify satisfaction of cybersecurity conditions of cipher information systems under such Committee.

4. Information systems critical for national security shall be commissioned for operation and use after they have been certified as satisfying cybersecurity conditions.

5. The Government shall provide detailed regulations for implementation of clause 2 above.

Article 13 *Inspections [audit] of cybersecurity of information systems critical for national security*

1. *An inspection [audit] of cybersecurity* means the activity of identifying the actual cybersecurity status of the information system and of its infrastructure or of information stored, processed and transmitted on it, aimed at preventing, detecting and dealing with any cybersecurity threat and proposing plans and measures to ensure normal operation of such system.

2. An audit of cybersecurity of an information system critical for national security shall be conducted in the following cases:

(a) When introducing e-facilities and network information security services for use in the information system;

(b) When there is a change in the current status of the information system;

(c) An annual inspection shall be conducted;

(d) A one-off inspection shall be conducted when there is a cybersecurity incident [breakdown] or an infringement of network security; or on request made by [a State administrative agency] for cybersecurity; or on expiry of the deadline for remedying any weaknesses or security vulnerabilities on the recommendation of a CTF.

3. Items subject to an inspection of cybersecurity of an information system critical for national security comprise:

(a) Hardware and software systems and digital devices used in the information system;

(b) Regulations and measures on protecting network security;

(c) Information which is stored, processed and transmitted on the information system;

(d) Plans of the system administrator to respond to and remedy any cybersecurity incident;

(dd) Measures for protecting State secrets and for preventing revelation or loss of State secrets via technical channels;

(e) Cybersecurity protective human resources.

4. The administrator of an information system critical for national security shall conduct cybersecurity inspections of the system within the managerial scope of such administrator in the cases prescribed in sub-clauses (a), (b) and (c) of clause 2 above; and shall provide written notice of the inspection results prior to October each year to the CTF under the Ministry of Public Security, or to such Task Force under the Ministry of National Defence in the case of a military information system.

5. One-off inspections of cybersecurity of an information system critical for national security are regulated as follows:

(a) Prior to the time for conducting an inspection, the CTF is responsible to provide at least twelve (12) hours advance written notice to the system administrator in the case of a cybersecurity incident or violation of cybersecurity, and at least 72 hours advance written notice in the case of a request [for inspection] made by a State administrative agency for cybersecurity or on expiry of the deadline for remedying any weaknesses or security vulnerabilities on the recommendation of a CTF;

(b) Within thirty (30) days after the day of ending an inspection, the CTF shall notify the inspection results and provide its requirements to the system administrator if any weaknesses or security vulnerabilities have been detected; and shall guide or participate in remedying [such defects] in the case where a proposal was made by the system administrator;

(c) The CTF under the Ministry of Public Security shall conduct one-off inspections of cybersecurity of information systems critical for national security, except for military information systems managed by the Ministry of National Defence, and except for cipher information systems under the Government Cipher Committee and cipher products which such Committee provides in order to protect information classified as State secret.

The CTF under the Ministry of National Defence shall conduct one-off inspections of cybersecurity of military information systems.

The Government Cipher Committee shall conduct one-off inspections of cybersecurity of cipher information systems managed by such Committee and of cipher products which such Committee provides in order to protect information classified as State secret;

(d) The administrator of an information system critical for national security is responsible to co-ordinate with the CTF to conduct the one-off inspection of cybersecurity.

6. The results of an inspection of cybersecurity must be kept confidential in accordance with law.

Article 14 *Supervision of cybersecurity of information systems critical for national security*

1. *Supervision of cybersecurity* means activities of collecting and analysing the current status so as to identify cybersecurity threats, cybersecurity incidents, any weaknesses or security vulnerabilities, malicious codes and malicious hardware in order to provide warnings thereof and remedy and deal with [such issues].

2. The administrator of an information system critical for national security shall preside over co-ordination with the competent CTF to regularly supervise cybersecurity of the system within the managerial scope of such administrator; and to formulate mechanisms for automatic warnings and receipt of such warnings of any cybersecurity threats, cybersecurity incidents, weaknesses or security vulnerabilities, malicious codes or malicious hardware in order to provide plans on emergency response and remedy.

3. The CTF shall supervise cybersecurity of information systems critical for national security within its managerial scope; and shall provide warnings and co-ordinate with the system administrator to remedy and deal with any cybersecurity threat, cybersecurity incident, weakness or security vulnerability, malicious code or malicious hardware in respect of the information system critical for national security.

Article 15 *Responding to and remedying any cybersecurity incident on an information system critical for national security*

1. Activities being response and remedying a cybersecurity incident on an information system critical for national security comprise:

(a) Detecting and identifying the cybersecurity incident;

(b) Protecting the site and collating evidence;

(c) Blockading and restricting the scope of the incident which has occurred, and mitigating loss and damage caused by it;

(d) Determining the objectives, objects and scope of the response;

(dd) Verifying, analysing, assessing and classifying such cybersecurity incident;

(e) Implementing plans on responding to and remedying the incident;

(g) Determining the cause of the incident and tracing its origin;

(h) Investigating and dealing with the incident in accordance with law.

2. The administrator of an information system critical for national security shall formulate a plan on addressing/responding to and remedying any cybersecurity incident on the system within the managerial scope of such administrator; and shall deploy such plan on occurrence of a cybersecurity incident and promptly report same to the competent CTF.

3. Coordination of the response and remedying any cybersecurity incident on an information system critical for national security is regulated as follows:

(a) The CTF under the Ministry of Public Security shall preside over coordination of activities of responding to and remedying any cybersecurity incident on an information system critical for national security, except in the cases prescribed in sub-clauses (b) and (c) below; shall participate in responding to and remedying a cybersecurity incident on an information system critical for national security when requested; and shall notify the system administrator on detection of a cyberattack or cybersecurity incident;

(b) The CTF under the Ministry of National Defence shall preside over coordination of activities responding to and remedying any cybersecurity incident occurring on a military information system;

(c) The Government Cipher Committee shall preside over coordination of activities of responding to and remedying any cybersecurity incident on a cipher information system under such Committee.

4. Agencies, organizations and individuals are responsible to participate in responding to and remedying any cybersecurity incident occurring on an information system critical for national security on request made by the force in charge of coordinating such response.

CHAPTER 3

Prevention of and Dealing with an Infringement of Cybersecurity

Article 16 *Prevention of and dealing with information in cyberspace with contents being propaganda against the Socialist Republic of Vietnam; information contents which incite riots, disrupt security or cause public disorder; which cause embarrassment or are slanderous; or which violate economic management order*

1. Information in cyberspace with contents being propaganda against the Socialist Republic of Vietnam comprises:

(a) Distortion or defamation of the people's administrative authorities;

(b) Psychological warfare, inciting an invasive war; causing division or hatred between [Vietnamese] ethnic groups, religions and people of all countries;

(c) Insulting the [Vietnamese] people, the national flag, national emblem, national anthem, great men, leaders, famous people or national heroes.

2. Information in cyberspace with contents inciting riots, disrupting security or causing public disorder comprises:

(a) Calling for, mobilizing, instigating, threatening or causing division, conducting armed activities or using violence to oppose the people's administrative authorities;

(b) Calling for, mobilizing, inciting, threatening, or embroiling a mass/crowd of people to disrupt or oppose people [officials] conducting their official duties, or obstructing the activities of agencies or organizations causing instability to security and order.

3. Information in cyberspace which causes embarrassment or which is slanderous comprises:

(a) Serious infringement of the honour, reputation/prestige or dignity of other people;

(b) Invented or untruthful information infringing the honour, reputation or dignity of other agencies, organizations or individuals or causing loss and damage to their lawful rights and interests.

4. Information in cyberspace which violates economic management order comprises:

(a) Invented or untruthful information about products, goods, money, bonds, bills, cheques and other valuable papers;

(b) Invented or untruthful information in the sectors of finance, banking, e-commerce, e-payment, currency trading, capital mobilization, multi-level trading and securities.

5. Information in cyberspace with invented or untruthful contents causing confusion amongst the Citizens, causing loss and damage to socio-economic activities, causing difficulties for the activities of State agencies or people performing their public duties [or] infringing the lawful rights and interests of other agencies, organizations and individuals.

6. The system administrator is responsible to implement managerial and technical measures in order to prevent, detect, stop and/or remove information with the contents prescribed in clauses 1 to 5 inclusive above on the system it administers when there is a request from the CTF.

7. The CTF and competent agencies shall apply the measures prescribed in sub-clauses (h), (i) and (l) of article 5.1 of this Law to deal with information in cyberspace with the contents prescribed in clauses 1 to 5 inclusive above.

8. Enterprises providing services on telecom networks, the Internet and other added value services on cyberspace and system administrators are responsible to coordinate with functional [State] agencies in dealing with information in cyberspace with the contents prescribed in clauses 1 to 5 inclusive above.

9. Organizations and individuals who compile, publish and disseminate information in cyberspace with the contents prescribed in clauses 1 to 5 inclusive above must remove it when so requested by a CTF and shall be liable [for same] in accordance with law.

Article 17 *Prevention of and combatting cyberespionage; and protection of information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace*

1. Conduct constituting cyberespionage; and infringement of State secrets, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace comprises:

(a) Appropriating, buying or selling, seizing and/or intentionally disclosing information classified as State secret or work secrets; business secrets, personal secrets, family secrets and private life [adversely] impacting on the honour, reputation, dignity and lawful rights and interests of agencies, organizations and individuals;

(b) Deliberately deleting, damaging, misplacing and/or changing information classified as State secret, or work secrets, business secrets, personal secrets, family secrets and private life which is transmitted and/or stored in cyberspace;

(c) Deliberately altering, cancelling or invalidating technical measures which have been constructed and/or applied in order to protect information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life;

(d) Putting in cyberspace information being State secret or work secrets, business secrets, personal secrets, family secrets and private life contrary to law;

(dd) Deliberately listening to or recording in sound or images conversations, contrary to law;

(e) Other acts of intentional infringement of State secrets, work secrets, business secrets, personal secrets, family secrets and private life.

2. System administrations have the following responsibilities:

(a) To inspect [audit] cybersecurity in order to detect and remove malicious codes and malicious hardware and to remedy security weaknesses and vulnerabilities; and to detect and deal with unlawful infringement activities or other threats to cybersecurity;

(b) To apply managerial and technical measures in order to prevent, detect and block any acts of cyberespionage, infringements of State secrets, work secrets, business secrets, personal secrets, family secrets or private life on the information system and to promptly remove any information related to such conduct;

(c) To coordinate with and implement requests made by the CTF regarding prevention and combatting cyberespionage and in order to protect information classified as State secret, work secrets, business secrets, personal secrets, family secrets or private life on the information system.

3. Agencies compiling and storing information and data classified as State secret are responsible to protect such State secret information which they have compiled and stored on computers or other equipment or exchanged in cyberspace, in accordance with the law on protection of State secrets.

4. The Ministry of Public Security has the following responsibilities, except for those prescribed in clauses 5 and 6:

(a) To inspect [audit] cybersecurity of information systems critical for national security in order to detect and remove malicious codes and malicious hardware, to remedy security weaknesses and vulnerabilities, and to discover, prevent and deal with unlawful acts of infringement;

(b) To inspect cybersecurity of communications equipment, products and services, digital equipment and of e-equipment prior to commissioning same for use on information systems critical for national security;

(c) To supervise cybersecurity of information systems critical for national security in order to detect and deal with activities of unlawfully gathering information classified as State secret;

(d) To detect and deal with unlawful acts of posting, storing or exchanging in cyberspace information and data containing contents classified as State secret;

(dd) To participate in research and manufacture of products which store and transmit information and data with contents classified as State secret; and products which code information in cyberspace in accordance with the functions and duties allocated [to such Ministry];

(e) To check and inspect the work of State agencies protecting State secrets in cyberspace and the work of cybersecurity protection by administrators of information systems critical for national security;

(g) To arrange training courses to raise the awareness of and knowledge on protection of State secrets in cyberspace, and on prevention of and combatting cyberattacks, and on cybersecurity protection for the cybersecurity task forces prescribed in article 30.2 of this Law.

5. The Ministry of National Defence is responsible to implement the items prescribed in sub-clauses (a), (b), (c), (d) and (dd) of clause 4 above with respect to military information systems.

6. The Government Cipher Committee is responsible to arrange implementation of provisions of the law on use of cryptography in order to protect information classified as State secret which is stored and exchanged in cyberspace.

Article 18 *Prevention of and combatting use of cyberspace, information technology and electronic media in order to breach the law on national security, social order and safety*

1. Conduct being the use of cyberspace, IT and electronic media in order to breach the law on national security, social order and safety comprises:

(a) Posting and/or disseminating information in cyberspace with the contents prescribed in clauses 1 to 5 of article 16 and the conduct prescribed in article 17.1 of this Law;

(b) Appropriating assets/property; organizing gambling including gambling via the Internet; stealing international telecom charges on the Internet; and breaching copyright and intellectual property rights in cyberspace;

(c) Falsifying websites of agencies, organizations or individuals; forging, circulating, stealing, buying or selling, collecting or exchanging unauthorized credit card information or bank accounts of other people; unlawfully issuing, providing or using payment means;

(d) Disseminating, advertising or purchasing and selling goods or services on the list of those prohibited by law;

(dd) Guiding other people to conduct acts in breach of law;

(e) Other acts of using cyberspace, IT or e-facilities to breach the law on national security, social order and safety.

2. Cybersecurity Task Forces are responsible to prevent and combat conduct being the use of cyberspace, IT, or e-facilities to breach the law on national security, social order and safety.

Article 19 *Prevention of and combating cyberattacks*

1. Acts constituting a cyberattack and cyberattack-related acts comprise:

(a) Distributing informatics programs which cause harm to a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility;

(b) Hindering, disordering, paralyzing, interrupting or stopping the operation of, and/or illegally preventing the transmission of data by a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility;

(c) Infiltrating, harming or appropriating data stored or transmitted on a telecom network, the Internet, a computer network, information systems, information processing and control systems, database or e-facility;

(d) Infiltrating, creating or exploiting security vulnerabilities or weaknesses and system services in order to appropriate information and/or to earn illicit profit;

(dd) Producing, purchasing and selling, exchanging or donating tools, devices [equipment] and software with the function of attacking a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility in order to use such objects [tools, devices and software] for illegal purposes;

(e) Performing other acts which affect the normal operation of any telecom network, the Internet, computer network, information system, information processing and control system, database or e-facility.

2. Information system administrators are responsible to apply technical measures to prevent and avoid the acts prescribed in sub-clauses (a), (b), (c), (d) and (e) of clause 1 above with respect to information systems within their managerial scope.

3. When a cyberattack occurs and infringes or threatens to infringe national sovereignty, interests and security and/or causes serious harm to social order and safety, the Cybersecurity Task Force shall preside over coordination with information system administrators and relevant organizations and individuals to apply measures to determine the origin of the cyberattack and collect evidence; and shall require enterprises providing services on telecom networks, the Internet and other added value services on cyberspace [cyberspace service providers] to block and filter information in order to prevent and eliminate acts of cyberattack, and shall promptly provide complete relevant information and data.

4. The responsibility to prevent and combat cyberattack is regulated as follows:

(a) The Ministry of Public Security shall preside over coordination with relevant Ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article which infringe or threaten to infringe national sovereignty, interests and security or cause serious harm to social order and safety throughout the entire country, except in the cases prescribed in sub-clauses (b) and (c) below;

(b) The Ministry of National Defence shall preside over coordination with relevant Ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to military information systems;

(c) The Government Cipher Committee shall preside over coordination with ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to cipher information systems under such Committee.

Article 20 *Prevention of and combating cyberterrorism*

1. Competent State agencies are responsible to apply measures stipulated in this Law, article 29 of the law on network information security and the law on prevention of and combating against terrorism, to deal with cyberterrorism.

2. Information system administrators shall regularly review and inspect information systems within their managerial scope in order to eliminate cyberterrorism threats.

3. Any agency, organization or individual which detects any indication or any act of cyberterrorism must promptly notify a CTF thereof. An agency receiving such notice is responsible to receive complete/full news of such cyberterrorism and promptly notify same to the CTF.

4. The Ministry of Public Security shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, to apply measures to neutralize cyberterrorism sources, to deal with cyberterrorism, and to minimize consequences occurring to information systems, except in the cases prescribed in clauses 5 and 6 of this article.

5. The Ministry of National Defence shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, and to apply measures to deal with cyberterrorism occurring to military information systems.

6. The Government Cipher Committee shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, and to apply measures to deal with cyberterrorism occurring to cipher information systems under such Committee.

Article 21 *Prevention of and dealing with dangerous cybersecurity situations*

1. Dangerous cybersecurity situations comprise:

(a) The presence of inciting information in cyberspace resulting in possible occurrence of riots, security disruption or terrorism;

(b) Attack on information systems critical for national security;

(c) Attack on a number of information systems on a large scale and of high strength;

(d) Attack on networks for the purpose of destroying important construction works regarding national security and important targets regarding national security;

(dd) Cyberattacks which seriously infringe national sovereignty, interests and security; or which cause very serious loss of social order and safety and the lawful rights and interests of agencies, organizations and individuals.

2. The responsibility to prevent dangerous cybersecurity situations is regulated as follows:

(a) The Cybersecurity Task Force shall coordinate with administrators of information systems critical for national security to implement technical solutions and professional activities to prevent, detect and deal with dangerous cybersecurity situations;

(b) Telecom, Internet and IT enterprises, enterprises providing services on telecom networks, the Internet and other added value services on cyberspace and relevant agencies, organizations and individuals are responsible to coordinate with the CTS under the Ministry of Public Security in preventing, detecting and dealing with dangerous cybersecurity situations.

3. The measures to deal with a dangerous cybersecurity situation comprise:

(a) Immediate implementation of emergency plans for prevention and response, and preventing, excluding or mitigating loss and damage caused by such dangerous situation;

(b) Sending a notice to relevant agencies, organizations and individuals;

(c) Collecting relevant information; and continuous monitoring and supervision of such dangerous situation;

(d) Analysing and assessing information about and forecasts of possible affects and the scope of affect and the level of loss and damage caused by such dangerous situation;

(dd) Ceasing provision of network information in specific areas or disconnecting international network gateways;

(e) Arranging forces and equipment to prevent and eliminate the dangerous situation;

(g) Other measures as stipulated in the *Law on National Security*.

4. A dangerous cybersecurity situation shall be dealt with as follows:

(a) Any agency, organization or individual which discovers a dangerous cybersecurity situation must promptly notify the CTF and immediately apply the measures prescribed in sub-clauses (a) and (b) of clause 3 above;

(b) The Prime Minister of the Government shall consider and make a decision on, or authorize the Minister of Public Security to consider and make a decision on dealing with any dangerous cybersecurity situation throughout the entire country or in each locality or for a specific target.

The Prime Minister of the Government shall consider and make a decision on, or authorize the Minister of National Defence to consider and make a decision on dealing with any dangerous cybersecurity situation occurring to military information systems and cipher information systems under the Government Cipher Committee;

(c) The CTF shall preside over coordination with relevant agencies, organizations and individuals to apply the measures prescribed in clause 3 above to deal with the dangerous cybersecurity situation;

(d) Relevant agencies, organizations and individuals are responsible to coordinate with the CTF to implement measures to prevent and deal with any dangerous cybersecurity situation.

Article 22 *Fighting to protect cybersecurity*

1. *Fighting to protect cybersecurity* means an organized activity conducted by a CTF in cyberspace in order to protect national security and ensure social order and safety.

2. Items of fighting to protect cybersecurity comprise:

(a) Keeping track of the situation relating to national security protective activities;

(b) Preventing and combating attacks, and protecting the stable operation of information systems critical for national security;

(c) Paralyzing or restricting the use of cyberspace when such use causes harm to national security or causes particularly serious harm to social order and safety;

(d) Proactively attacking and neutralizing targets in cyberspace in order to protect national security and ensure social order and safety.

3. The Ministry of Public Security shall preside over coordination with relevant Ministries and line ministries in fighting to protect cybersecurity.

CHAPTER 4

Cybersecurity Protective Activities

Article 23 *Implementation of cybersecurity protective activities in State agencies and political organizations at the central and local levels*

1. Contents of implementation of cybersecurity protective activities comprise:

(a) Formulating and completing rules and regulations on use of local area networks and Internet-connected computer networks; plans for ensuring cybersecurity of information systems; and plans for responding to and remedying cybersecurity incidents;

(b) Applying and implementing plans, measures and technology to protect cybersecurity of information systems and of information and data archived, drafted and transmitted on information systems within the scope of their managerial authority [managed by such State agencies and political organizations];

(c) Organizing retraining on cybersecurity knowledge for cadres [senior officials], other officials and employees; increasing the capability of Cybersecurity Task Forces [CTF] to protect cybersecurity;

(d) Protecting cybersecurity in the following activities: providing public services in cyberspace; providing information to, exchanging information with and collecting information from agencies, organizations and individuals; sharing information internally and with other agencies or during other activities in accordance with Government regulations;

(dd) Conducting investment in and building physical infrastructure in conformity with conditions for ensuring implementation of cybersecurity protective activities for information systems;

(e) Inspecting cybersecurity of information systems; preventing and combating breaches of the law on cybersecurity; responding to and remedying cybersecurity incidents.

2. Heads of agencies and organizations are responsible to carry out cybersecurity protective activities [for networks] within the scope of their managerial authority.

Article 24 *Inspection [audit] of cybersecurity of information systems of agencies and organizations not on the list of information systems critical for national security*

1. Cybersecurity of information systems of agencies and organizations not on the list of information systems critical for national security shall be inspected in the following cases:

(a) When there is a breach of the law on cybersecurity infringing national security or materially affecting social order and safety;

(b) When there is a request from the information system administrator.

2. Items subject to cybersecurity inspection comprise:

(a) Hardware and software systems and digital devices used in the information system;

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

(c) Measures for protecting State secrets, and for preventing and combating revelation and loss of State secrets via technical channels.

3. An information system administrator is responsible to notify the CTF under the Ministry of Public Security upon discovery of any breach of the law on cybersecurity on an information system within the scope of his/her managerial authority.

4. The CTF under the Ministry of Public Security shall conduct inspections of cybersecurity of information systems of agencies and organizations in the cases prescribed in clause 1 of this article.

5. The CTF shall provide [advance] written notice to the information system administrator at least twelve (12) hours prior to the time of conducting an inspection.

   The CTF shall, within thirty (30) days after the end date of an inspection or audit, notify the inspection results and provide requirements to the information system administrator if any security weakness or vulnerabilities are discovered; and shall provide guidelines for or participate in remedying [such weakness or vulnerabilities] pursuant to a request from the information system administrator.

6. Results of cybersecurity inspection shall be kept confidential in accordance with law.

7. The Government shall stipulate the sequence and procedures for cybersecurity inspections prescribed in this article.

Article 25 *Protection of cybersecurity of national cyberspace infrastructure and international network gateways*

1. The protection of cybersecurity of the national cyberspace infrastructure and international network gateways must closely combine requirements on cybersecurity protection with requirements on socio-economic construction and development; international network gateways are encouraged to be located within the territory of Vietnam; and organizations and individuals are encouraged to participate in investment in building national cyberspace infrastructure.

2. Agencies, organizations and individuals managing and operating national cyberspace infrastructure and international network gateways have the following responsibilities:

(a) To protect cybersecurity within the scope of their managerial authority; to be subject to management, investigation and inspection by, and to comply with requirements on cybersecurity protection of competent State agencies;

(b) To facilitate and implement necessary technical measures and professional activities when requested in order for competent State agencies to perform cybersecurity protective tasks.

Article 26 *Guarantees relating to information security in cyberspace*

1. Websites, portals [and] specialized pages on social networks of agencies, organizations and individuals must not provide, upload or transmit any information with the contents prescribed in clauses 1 to 5 of article 16 of this Law and other information containing contents infringing national security.

2. Any domestic or foreign enterprise which provides services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [*cyberspace service provider*] has the following responsibilities:

(a) To authenticate information when a user registers a digital account; to maintain confidentiality of information and accounts of users; to provide user information to the Cybersecurity Task Force under the Ministry of Public Security when so requested in writing in order to serve investigation of and dealing with breaches of the law on cybersecurity;

(b) To prevent the sharing of information and to delete information with the contents prescribed in clauses 1 to 5 inclusive of article 16 of this Law on services or information systems directly managed

by any agency or organization no later than twenty four (24) hours after the time of a request from the CTF under the Ministry of Public Security or from a competent agency under the Ministry of Information and Communications, and to save/maintain system logs in order to serve investigation of and dealing with breaches of the law on cybersecurity within a [specified] period [to be] stipulated by the Government;

(c) Not to provide or to cease provision of services on telecom networks and on the Internet and other value added services to organizations and individuals who upload in cyberspace information with the contents prescribed in clauses 1 to 5 of article 16 of this Law, when requested by the CTF under the Ministry of Public Security or by a competent agency under the Ministry of Information and Communications.

3. Domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [*cyberspace service providers*] carrying out activities of collecting, exploiting [using], analysing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government.

Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam.

4. The Government shall provide detailed regulations on clause 3 of this article.

Article 27 *Research and development of cybersecurity*

1. Contents of research and development of cybersecurity comprise:

(a) Establishment of systems of cybersecurity protective software and equipment;

(b) Methods of evaluating whether cybersecurity software and equipment satisfy standards, and minimizing the existence of security vulnerabilities or weaknesses, and malware;

(c) Methods of checking whether the hardware and software which is provided in fact functions properly;

(d) Methods of protecting State secrets, work-related secrets, business secrets, personal secrets, family secrets and private life [personal privacy], and the capability of maintaining confidentiality when transmitting information in cyberspace;

(dd) Determination of the sources of information transmitted in cyberspace;

(e) Resolution of cybersecurity threats;

(g) Establishment of the network range and the cybersecurity testing environment;

(h) Technical initiatives increasing cybersecurity awareness and skills;

(i) Cybersecurity forecasts;

(k) Practical research and theoretical development of cybersecurity.

2. Relevant agencies, organizations and individuals have the right to research and develop cybersecurity.

Article 28 *Improvement of self-autonomy regarding cybersecurity*

1. The State encourages and facilitates agencies, organizations and individuals to improve their self-autonomy regarding cybersecurity and to increase the productivity, inspection, assessment and testing of digital devices, network services and network applications.

2. The Government shall implement the following measures in order to improve self-autonomy of agencies, organizations and individuals regarding cybersecurity:

(a) Promoting transfer, research, control [ability to master/own] and development of technology, products, services and applications in order to protect cybersecurity;

(b) Promoting application of new technology and advanced technology relating to cybersecurity;

(c) Training, and developing and using [employing] cybersecurity human resources;

(d) Strengthening the business environment and improving competitive conditions in order to assist enterprises to research and produce products, services and applications for the purpose of cybersecurity protection.

Article 29 *Child protection in cyberspace*

1. Children have the right to be protected; to access information; to participate in social, entertainment and recreational activities; to keep their personal secrets confidential, and other rights when they participate in cyberspace.

2. Information system administrators and cyberspace service providers are responsible to control information on [their] information systems or on services provided by them, in order not to cause harm to or mistreatment of children or infringing children's rights; and to block the sharing of and to delete information the contents of which may cause harm to or mistreat children or infringe their rights; and [are responsible to] promptly notify and co-ordinate with the CTF under the Ministry of Public Security for resolution.

3. Agencies, organizations and individuals participating in activities in cyberspace are responsible to co-ordinate with competent State administrative agencies to guarantee children's rights in cyberspace, and prevent [block] network information with contents causing harm to children, in accordance with this Law and the law on children.

4. Agencies, organizations, parents, teachers, child carers and other relevant individuals are responsible to guarantee children's rights and to protect children in accordance with the law on children when they [the former] participate in cyberspace.

5. Cybersecurity Task Forces and functional agencies are responsible to take measures to preclude, discover, prevent and strictly deal with the use of cyberspace to cause harm to or intrude on children or to infringe their rights.

CHAPTER 5

Guarantees Relating to Cybersecurity Protective Activities

Article 30 *Cybersecurity protective forces [comprise:]*

1. Cybersecurity Task Forces [CTFs] to be arranged under the Ministry of Public Security and the Ministry of Defence.

2. Other cybersecurity task forces to be arranged under ministries, branches, provincial people's committees, agencies and organizations which directly manage information systems critical for national security.

3. Organizations and individuals mobilized to participate in cybersecurity protection.

Article 31 *Guarantees relating to cybersecurity protective human resources*

1. Vietnamese Citizens who have knowledge of cybersecurity, network information safety and IT shall provide the fundamental and main human resource for protecting cybersecurity.

2. The State shall formulate programs and plans for forming and developing human resources for cybersecurity protection.

3. Upon occurrence of any dangerous situation in respect of cybersecurity, cyberterrorism, a cyberattack, a cybersecurity incident or cybersecurity threat, the competent State administrative agencies shall issue a decision mobilizing cybersecurity protective human resources.

   The authority, responsibility, sequence and procedures for mobilizing cybersecurity protective human resources shall accord with the *Law on National Security*, the *Law on National Defence*, the *Law on People's Public Security* and other relevant laws.

Article 32 *Selection, training and development of cybersecurity protective forces*

1. Any Vietnamese citizen who satisfies all the standards on ethics, health, [professional] qualifications; knowledge of cybersecurity, network information safety and IT; and who expresses readiness may be selected to join the cybersecurity protective forces.

2. Prioritized training and development of high-quality cybersecurity protective forces.

3. Prioritized development of cybersecurity training establishments which satisfy international standards; and encouraged association of, and facilitated co-operation on cybersecurity between the State sector and the private sector both domestic and foreign.

Article 33 *Education and retraining on cybersecurity knowledge and activities*

1. Contents of education and retraining on cybersecurity knowledge shall be presented in the subject of national defence and security taught at schools and in programs on retraining on national defence and security knowledge in accordance with the *Law on Education on National Defence and Security*.

2. The Ministry of Public Security shall preside over co-ordination with relevant ministries and branches to organize retraining on cybersecurity activities for the CTF and for officials and employees who participate in protecting cybersecurity.

   The Ministry of Defence and the Government Cipher Department shall organize retraining on cybersecurity activities for entities within their managerial scope.

Article 34 *Dissemination of knowledge about cybersecurity*

1. The State formulates policies for dissemination of knowledge about cybersecurity throughout the entire country and encourages State agencies to coordinate with private organizations and individuals to implement educational programs and to increase awareness of cybersecurity.

2. Ministries, branches, agencies and organizations are responsible to formulate and implement activities of disseminating cybersecurity knowledge to their senior officials, other officials and employees.

3. Provincial people's committees are responsible to formulate and implement activities of disseminating knowledge about, and increasing awareness of cybersecurity for local agencies, organizations and individuals.

Article 35 *Funds for the guarantees relating to cybersecurity protective activities*

1. Funds for cybersecurity protective activities of State agencies and political organizations shall be guaranteed by the State Budget and arranged in the annual State budget estimate. The management and use of State Budget funds shall accord with the law on State budget.

2. Funds for implementing cybersecurity protective activities for the information systems of agencies and organizations other than those prescribed in clause 1 above shall be guaranteed by such agencies and organizations.

CHAPTER 6

Responsibilities of Agencies, Organizations and Individuals

Article 36 *Responsibilities of the Ministry of Public Security*

The Ministry of Public Security is liable before the Government to exercise State administration of cybersecurity with the following duties and powers, except for matters which are the responsibility of the Ministry of Defence and the Government Cipher Department:

1. To promulgate or submit to the competent State agency to promulgate legal instruments on cybersecurity including implementing guidelines.

2. To formulate and propose strategies, guidelines, policies, plans and options for cybersecurity protection.

3. To prevent and combat the use of cyberspace to infringe national sovereignty, interests and security, social order and safety; and to prevent and combat cybercrime.

4. To protect security of information in cyberspace; to formulate mechanisms to authenticate information [used to] register digital accounts; to give warnings about cybersecurity threats and to share cybersecurity information.

5. To consult with and propose that the Government and the Prime Minister consider and decide on allocation and co-ordination to implement measures for cybersecurity protection and to prevent or deal with cybersecurity infringement if multiple ministries and branches exercise State administration of the relevant items.

6. To organize drills to prevent and combat cyberattacks; to carry out drills to respond to and remedy cybersecurity incidents occurring within any information system critical for national security.

7. To conduct inspections and investigations, resolve complaints and denunciations, and deal with breaches of the law on cybersecurity.

Article 37 *Responsibilities of the Ministry of National Defence*

The Ministry of National Defence is liable before the Government to exercise State administration of cybersecurity within its managerial scope and has the following duties and powers:

1. To promulgate or submit to the competent State agency to promulgate legal instruments on cybersecurity including implementing guidelines on matters within its managerial scope.

2. To formulate and propose strategies, guidelines, policies, plans and options for cybersecurity protection on matters within its managerial scope.

3. To prevent and combat, within its managerial scope, the use of cyberspace to infringe national security.

4. To co-ordinate with the Ministry of Public Security to organize drills to prevent and combat cyberattacks; to carry out drills to respond to and remedy cybersecurity incidents within any information system critical for national security; and to commence implementation of cybersecurity protective work.

5. To conduct inspections and investigations, resolve complaints and denunciations, and deal with breaches of the law on cybersecurity within its managerial scope.

Article 38 *Responsibilities of the Ministry of Information and Communications*

1. To co-ordinate with the Ministry of Public Security and the Ministry of National Defence in protecting cybersecurity.

2. To co-ordinate with relevant agencies to disseminate [educate about the dangers of] and to counter information which opposes the Socialist Republic of Vietnam as prescribed in article 16.1 of this Law.

3. To request cyberspace service providers and information system administrators to remove information in breach of the law on cybersecurity from the services and information systems directly managed by enterprises, agencies or organizations.

Article 39 *Responsibilities of the Government Cipher Department*

1. To consult with and propose that the Ministry of National Defence promulgate or submit to the competent agency to promulgate and organize implementation of legal instruments, programs and plans on cryptography in order protect cybersecurity within the managerial scope of such Department.

2. To protect cybersecurity of the cipher information system of the Government Cipher Department and cryptographic products provided by such Department in accordance with this Law.

3. To uniformly manage science and technology research on cryptography; and to produce, use and provide cryptographic products in order to protect information stored or exchanged in cyberspace which is State secret.

Article 40 *Responsibilities of ministries, branches and provincial people's committees*

Ministries, branches and provincial people's committees shall, depending on their respective duties and powers, protect cybersecurity of information and information systems within their managerial scope; and shall co-ordinate with the Ministry of Public Security to exercise State administration of cybersecurity of such ministries, branches and localities.

Article 41 *Responsibilities of service providers in cyberspace*

1. A cyberspace service provider[4] in Vietnam has the following responsibilities:

(a) To give warnings of the possibility of a loss of cybersecurity during use of the services in cyberspace provided by such enterprise and to provide guidelines on preventive measures;

(b) To formulate plans and solutions to quickly respond to cybersecurity incidents, and to immediately deal with any security weaknesses or vulnerabilities, malicious codes, cyberattacks, cyber intrusions/infringements or other security risks; and when a cybersecurity incident occurs, to immediately implement appropriate emergency plans and response measures, and at the same time provide a report thereon to the CTF in accordance with this Law;

(c) To apply technical solutions and other necessary measures to ensure security during the process of collecting information and to prevent the risk of revelation, damage to or loss of data; and in the case

[4] Allens footnote: The literal translation is "An enterprise providing services in cyberspace".

of occurrence or possible occurrence of the revelation, damage to or loss of data about user information, to immediately provide response solutions, and at the same time notify the user and report to the CTF in accordance with this Law;

(d) To co-ordinate with and facilitate CTFs to conduct their cybersecurity protective activities.

2. Cyberspace service providers in Vietnam are responsible to implement the provisions in clause 1 of this article and clauses 2 and 3 of articles 26 of this Law.

Article 42 *Responsibilities of agencies, organizations and individuals using cyberspace*

1. To comply with the law on cybersecurity.

2. To promptly provide information relating to cybersecurity protection, cybersecurity threats and any cybersecurity intrusion/infringement to the competent agency and CTF.

3. To implement requirements and guidelines of competent agencies during cybersecurity protection; to assist and facilitate agencies, organizations and responsible persons to implement measures for cybersecurity protection.

CHAPTER 7

Implementing Provisions

Article 43 *Effectiveness*

1. This Law is of full force and effect as from 1 January 2019.

2. With respect to information systems under operation and in use and on the list of information systems critical for national security, within twelve (12) months from the effective date of this Law, the information system administrators are responsible to ensure satisfaction of all of the conditions on cybersecurity, and a Cybersecurity Task Force shall assess the conditions on cybersecurity in accordance with article 12 of this Law; any extension required shall be decided by the Prime Minister, but not to exceed twelve (12) months.

3. With respect to information systems under operation and in use which are added to the list of information systems critical for national security, within twelve (12) months from the date of addition, the information system administrators are responsible to ensure satisfaction of all of the conditions on cybersecurity, and a Cybersecurity Task Force shall assess the conditions on cybersecurity in accordance with article 12 of this Law; any extension required shall be decided by the Prime Minister, but not to exceed twelve (12) months.

This Law was passed by Legislature XIV of the National Assembly of the Socialist Republic of Vietnam at the 5th session on 12 June 2018.

Chairwoman of the National Assembly

NGUYEN THI KIM NGAN