

HO CHI MINH NATIONAL ACADEMY OF POLITICS

BUI THI THUY DUNG

**IMPROVING THE LAW ON
CYBERSECURITY IN VIETNAM**

SUMMARY OF DOCTORAL THESIS

MAJOR: THEORY AND HISTORY OF STATE AND LAW

Code: 9380106

HANOI - 2026

The research is completed at Ho Chi Minh National Academy of Politics

***Academic Supervisors:* 1. Assoc. Prof. Dr. Bui Thi Hanh**



2. Assoc. Prof. Dr. Nguyen Thi Tuyet Mai



Reviewer 1:

.....

Reviewer 2:

.....

Reviewer 3:

.....

**The thesis will be defended before the Academy-level Thesis Evaluation
Council held at Ho Chi Minh National Academy of Politics**

At hour date month year 2026

**The thesis is available for reference at: The National Library and
the Library of Ho Chi Minh National Academy of Politics**

INTRODUCTION

1. Rationale

In the current context, alongside the robust development of digital technology, the Internet, and connectivity platforms, cyberspace has become an essential environment for the operations of the State, the economy, and social life. Given the advancement of artificial intelligence, big data, cloud computing, the Internet of Things, and cross-border digital platforms, cybersecurity is approached not solely as an issue of technical protection for information systems but also as a political - legal matter inherently linked to the safeguarding of national security, social order and safety, digital sovereignty, human rights, civil rights, and sustainable development.

In Vietnam, the process of developing e-Government, digital government, digital economy, and digital society has established critical premises for national development. Consequently, cyberspace has evolved into a vital and sensitive domain, concentrating numerous threats that compromise national security and the legitimate rights and interests of agencies, organizations, and individuals. Cognizant of this imperative, the Party and the State of Vietnam have promulgated various strategic guidelines and directives regarding the defense of the Fatherland in cyberspace, ensuring cybersecurity, and promoting digital transformation. In recent years, our State has enacted significant legal documents such as the Law on Network Information Security in 2015, the Law on Cybersecurity in 2018, and implementing guidelines.

However, the rapid practical evolution of technology and cyberspace necessitates a continued comprehensive, systematic, and more profound research on cybersecurity law. Derived from the aforementioned analyses, researching the topic “Improving the law on cybersecurity in Vietnam” is an objective, urgent requirement of strategic significance.

2. Research Objectives and Tasks

2.1. Research Objectives

The research objective of the thesis is to build a solid theoretical foundation and establish a set of criteria to evaluate the degree of perfection of the cybersecurity law in Vietnam. Based on this, the thesis conducts an analysis of the current legal reality, identifies advantages, limitations,

inadequacies, and their causes, thereby proposing orientations and solutions for legal improvement to enhance the effectiveness of cybersecurity protection in the context of digital transformation and international integration. Adopting a risk governance approach to improving cybersecurity law, the thesis emphasizes the necessity of developing a legal system that ensures both the effectiveness of national security protection and transparency, feasibility, and the control of state power in the digital environment.

2.2. Research Tasks

To achieve the above objectives, the thesis performs the following primary tasks:

First, to review and evaluate relevant domestic and international research works, thereby identifying research gaps, research questions, and research hypotheses.

Second, to build the theoretical foundation of cybersecurity law and its improvement; to elucidate the concept, characteristics, role, scope, structure, and content of cybersecurity law in Vietnam.

Third, to establish a set of criteria for evaluating the degree of perfection of the cybersecurity law, including criteria concerning legal content, legislative techniques, and law enforcement.

Fourth, to investigate the experience in formulating cybersecurity law of selected countries, regions, and international organizations to derive applicable reference values for Vietnam.

Fifth, to analyze and evaluate the reality of the law and the practical enforcement of cybersecurity law in Vietnam based on the established criteria and fundamental institutional groups; to point out advantages, limitations, inadequacies, and causes.

Sixth, to propose orientations and solutions for improving the law on cybersecurity in Vietnam.

3. Object and Scope of the Research

3.1. Object of the Research

The research object of the thesis is the law on cybersecurity in Vietnam from the perspective of the Theory and History of State and Law discipline. The thesis studies six fundamental institutional groups of cybersecurity law,

including: principles of cybersecurity protection; acts violating cybersecurity law; sanctions against violating acts; legal status of subjects; measures for cybersecurity protection; international cooperation in the field of cybersecurity.

3.2. Scope of the Research

Regarding content, the thesis focuses on studying the law on cybersecurity in Vietnam across six fundamental institutional groups and evaluating it against criteria of legal content, legislative techniques, and law enforcement. Regarding spatial scope, the thesis studies cybersecurity law in Vietnam; simultaneously, it selectively investigates the laws and experiences of certain countries, regions, and international organizations holding reference values for Vietnam, such as the United States, the European Union, the Russian Federation, China, Singapore, and relevant international cooperation mechanisms in cybersecurity. Regarding temporal scope, the thesis studies the legal system and the practical application of cybersecurity law in Vietnam from the promulgation of the Law on Network Information Security in 2015 and the Law on Cybersecurity in 2018 to the end of 2025.

4. Theoretical Basis and Research Methods

4.1. Theoretical Basis

The thesis is researched based on the theoretical foundation of Marxism-Leninism, Ho Chi Minh's thought on State and Law; the 2013 Constitution of the Socialist Republic of Vietnam, amended and supplemented in 2025; treaties and agreements to which Vietnam is a signatory or participant; the Party's directing viewpoints and the State's policies on protecting national security, ensuring social order and safety, protecting human rights and civil rights, building the socialist rule-of-law State of Vietnam, and developing a safe and healthy cyberspace.

4.2. Methodology and Research Methods

The thesis is conducted based on the methodology of dialectical materialism and historical materialism, positioning cybersecurity law within the dynamic relationship between the requirements of protecting national security, ensuring social order and safety, protecting human rights and civil rights, and the requirement of developing a safe and healthy cyberspace. Building upon this methodology, the thesis utilizes a combination of research

methods: legal norm analysis method; systematization and synthesis method; legal-historical method; comparative law method; case study and situational analysis method; descriptive statistics and secondary data processing method; expert interview and discussion method. In addition to traditional legal research methods, the thesis employs expert interviews and discussions to verify, supplement, and deepen the assessments of the legal reality, practical law enforcement, and the feasibility of solutions for improving cybersecurity law.

5. New Scientific Contributions of the Thesis

The thesis offers several new scientific contributions as follows:

The thesis clarifies the concept, characteristics, role, and content of cybersecurity law, establishing a scientific basis to evaluate the degree of perfection of this legal domain; analyzes the current legal system according to fundamental institutional groups, identifying legal loopholes, overlaps, inconsistencies, and limitations in the enforcement mechanism. Consequently, it proposes orientations and solutions to improve cybersecurity law in Vietnam. The thesis constructs the structure of cybersecurity law into six fundamental institutional groups, including: principles of cybersecurity protection; acts violating cybersecurity law; sanctions against violating acts; legal status of subjects; measures for cybersecurity protection; international cooperation in the field of cybersecurity.

The thesis elucidates the new requirements posed for the improvement of cybersecurity law in the context of digital transformation, the development of the digital economy, digital data, artificial intelligence, and international integration.

6. Theoretical and Practical Significance of the Thesis

6.1. Theoretical Significance

The thesis contributes to systematizing and clarifying the theoretical basis of cybersecurity law, the criteria for evaluating the degree of legal perfection, and the conditions assuring the improvement of cybersecurity law. The thesis also studies the experience of cybersecurity law from selected countries, regions, and international organizations, thereby highlighting valuable reference points for Vietnam. Furthermore, the thesis systematizes and analyzes the inadequacies and shortcomings within the six major institutional groups of

cybersecurity law; simultaneously, it identifies and explicates solutions for improving and ensuring the effective enforcement of cybersecurity law in the current context of Vietnam.

6.2. Practical Significance

The thesis serves as a valuable reference material for subjects undertaking tasks of legislation, regulation, state management, building and organizing the enforcement of cybersecurity law in Vietnam, particularly during the process of amending, supplementing, and promulgating relevant normative legal documents. Additionally, the thesis can be utilized as academic and reference material in training, fostering, and researching cybersecurity law, state management in cyberspace, and cybersecurity assurance tasks at relevant agencies and organizations.

7. Structure of the Thesis

In addition to the introduction, conclusion, appendices, and reference list, the content of the thesis is structured into 04 chapters, comprising 14 sections.

Chapter 1

OVERVIEW OF THE RESEARCH SITUATION RELATED TO THE THESIS TOPIC

1.1. RESEARCH WORKS RELATED TO THE THESIS TOPIC

1.1.1. Theoretical research works on improving cybersecurity law

Theoretical research works on improving cybersecurity law, both domestic and foreign, have provided a general theoretical foundation for legal improvement, especially criteria such as completeness, synchronicity, consistency, feasibility, transparency, suitability, and legislative techniques. The thesis inherits the general criteria system for legal improvement while developing these criteria to align with the specific characteristics of cybersecurity law.

1.1.2. Practical research works on improving cybersecurity law

Practical research works on improving cybersecurity law, both domestic and foreign, have explicitly indicated the role of cybersecurity in protecting national security, digital sovereignty, social order and safety, and

national interests in cyberspace. However, the thesis needs to further develop towards balancing the requirement of protecting national security with the requirement of protecting the legitimate rights and interests of individuals and organizations within a rule-of-law State.

1.1.3. Scientific works researching solutions to improve cybersecurity law

Research works on solutions to improve cybersecurity law, both domestic and foreign, have identified types of violating acts, characteristics of cybercrime, difficulties in investigation, evidence collection, jurisdiction determination, and handling cross-border acts. However, the thesis needs to systematically evaluate the relationship between violating acts, sanctions, cybersecurity protection measures, the legal status of subjects, and enforcement mechanisms within a holistic cybersecurity legal framework. Therefore, the thesis needs to analyze these issues according to the six identified institutional groups.

1.2. OVERVIEW OF RESEARCH RESULTS RELATED TO THE THESIS TOPIC AND EMERGING ISSUES

1.2.1. Overview of research results related to the thesis topic

Through studying and surveying domestic and foreign scientific works related to the topic, the PhD candidate draws several assessments as follows:

Issues that have been relatively clearly and specifically resolved by previous studies: established a general theoretical foundation for evaluating legal quality, particularly criteria regarding completeness, synchronicity, consistency, feasibility, transparency, and legislative techniques.

Issues that have not been fully resolved by previous studies: the scope of cybersecurity law vis-à-vis adjacent legal domains has not been distinctly demarcated; a specialized set of criteria to evaluate the degree of perfection of cybersecurity law has not been developed; there is a lack of connection between normative analysis and enforcement analysis; solutions in many works remain as general orientations, not closely tied to limitations, causes, and evaluation criteria.

Issues subject to ongoing debate and inconsistency in studies: regarding the scope of cybersecurity; the relationship between security protection and the protection of human rights and civil rights; the legal regulation model.

1.2.2. Issues the thesis needs to continue researching

Including: Concepts and scope of research; framework of evaluation criteria; structure of cybersecurity law; analysis of law enforcement; improvement solutions.

1.3. RESEARCH HYPOTHESIS AND QUESTIONS

1.3.1. Research Hypothesis

If the legal system on cybersecurity is improved towards synchronicity, feasibility, transparency, adaptability to technology, and ensures a balance between the requirement of protecting national security and protecting the legitimate rights and interests of individuals and organizations, then the effectiveness of state management and cybersecurity protection in Vietnam will be enhanced.

1.3.2. Research Questions

The overarching research question is: According to which criteria, contents, and enforcement mechanisms should the cybersecurity law in Vietnam be improved to ensure completeness, synchronicity, feasibility, transparency, and adaptability to the rapid development of digital technology, while balancing the requirement of protecting national security with the protection of the legitimate rights and interests of individuals and organizations in cyberspace?

The specific research questions are: (1) How should the theoretical basis and criteria for evaluating the degree of perfection of cybersecurity law be established? (2) What limitations is the cybersecurity law in Vietnam currently manifesting? (3) According to which orientations, solution groups, and specific legal designs should the cybersecurity law in Vietnam be improved?

Chapter 2

THEORETICAL BASIS OF IMPROVING THE LAW ON CYBERSECURITY

2.1. THEORETICAL FRAMEWORK FOR RESEARCHING CYBERSECURITY LAW

2.1.1. Basis for establishing the theoretical framework for researching cybersecurity law

The broadened security theory and securitization theory by Barry Buzan, Ole Wæver, and Jaap de Wilde serve as an important theoretical fulcrum for recognizing cybersecurity as a form of non-traditional security.

The theory of digital sovereignty and Internet control argues that cyberspace is not an entirely “territory-free” space or beyond the jurisdiction of the State.

Lawrence Lessig's “code is law” and architectural regulation theory in *Code and Other Laws of Cyberspace* indicates that behavior in cyberspace is regulated not only by law but also by social norms, markets, and technical architecture.

Ulrich Beck's risk society theory in the work *Risk Society: Towards a New Modernity*.

Daniel J. Solove's theory of privacy, surveillance, and the rule-of-law state in a technological environment.

Additionally, Mireille Hildebrandt's theory of the rule-of-law state in a technological environment.

2.1.2. Integrated theoretical framework for researching cybersecurity law

The thesis selects an integrated theoretical framework, combining the broadened security theory, digital sovereignty theory, architectural regulation theory, risk society theory, privacy theory, and the rule-of-law state in a technological environment theory to research cybersecurity law.

2.2. CONCEPT, LEGAL CHARACTERISTICS, ROLE, AND THEORETICAL STRUCTURE OF CYBERSECURITY LAW IN VIETNAM

2.2.1. Concept of cybersecurity law

Cybersecurity law is the totality of legal norms promulgated or recognized by the State, regulating social relations arising in the activities of protecting national security, social order and safety, information systems, data, and the legitimate rights and interests of agencies, organizations, and

individuals in cyberspace; through the establishment of cybersecurity protection principles, violating acts, sanctions, the legal status of subjects, cybersecurity protection measures, coordination mechanisms, and international cooperation; while placing the application of cybersecurity protection measures within the limits of the Constitution, the law, accountability, and the requirements of protecting human rights and civil rights.

This concept reveals several fundamental connotations of cybersecurity law.

First, cybersecurity law is a component of the national legal system, promulgated or recognized by the State, and guaranteed for implementation by state power.

Second, cybersecurity law aims to simultaneously protect multiple critical legal interests, including national security, social order and safety, information systems, data, and the legitimate rights and interests of agencies, organizations, and individuals.

Third, cybersecurity law comprises not only regulations on prohibited acts and sanctions but also regulations on principles, subjects, preventive measures, risk governance, coordination mechanisms, enforcement mechanisms, and international cooperation.

Fourth, cybersecurity law must be situated within the framework of the rule-of-law State.

2.2.2. Legal characteristics of cybersecurity law

2.2.2.1. *Interdisciplinary nature:* Legal regulations on cybersecurity govern not only the behavior of individuals and organizations in cyberspace but also establish the responsibilities of state agencies, specialized forces, information system administrators, service-providing enterprises, data processing organizations, and service users.

2.2.2.2. *High adaptability to technology:* The characteristic of high adaptability to technology also requires cybersecurity law to possess mechanisms for updating technical standards and regulations in areas such as information system protection, data protection, electronic tracing, encryption, identification, authentication, cybersecurity monitoring, incident reporting, incident response, and system recovery.

2.2.2.3. *Preventive and risk governance nature:* The preventive nature of cybersecurity law is primarily manifested in regulations on risk

assessment, information system classification, cybersecurity inspection, cybersecurity monitoring, threat warning, incident response exercises, critical information system protection, and the requirement to apply technical standards and regulations on information safety and security.

2.2.2.4. *Cross-border nature:* The cross-border characteristic of cybersecurity law is also evident in the fact that many entities playing a significant role in cybersecurity protection do not have their headquarters or technical infrastructure located in Vietnam, yet provide services to users in Vietnam.

2.2.2.5. *Multi-subject nature in enforcement:* Besides the State, service-providing enterprises in cyberspace constitute a particularly important group of subjects in the enforcement of cybersecurity law, information system administrators, and organizations/individuals using cyberspace are both subjects protected by law and subjects obliged to comply with cybersecurity law.

2.2.2.6. *Balance between protecting national security and protecting human rights and civil rights:* A characteristic of cybersecurity law is the perpetual necessity to manage the relationship between the requirement of protecting national security and social order and safety, and the requirement of protecting human rights, civil rights, and the legitimate rights and interests of individuals and organizations in cyberspace.

2.2.3. Role of cybersecurity law

2.2.3.1. Cybersecurity law is a tool to protect national security, ensure social order and safety, and protect national sovereignty in cyberspace and critical information systems: Cybersecurity law plays an especially critical role in protecting national security, national sovereignty in cyberspace, social order and safety, and critical information systems.

2.2.3.2. Cybersecurity law is a tool to protect the legitimate rights and interests of individuals and organizations in the digital environment: Cybersecurity law is not only a tool for protecting national security and social order and safety but also plays a vital role in protecting the legitimate rights and interests of individuals and organizations in the digital environment.

2.2.3.3. Cybersecurity law establishes the foundation for technology risk governance: Cybersecurity law plays an important role in establishing the legal basis for technology risk governance in the digital environment.

2.2.3.4. Cybersecurity law creates the legal foundation for a safe, transparent, and sustainable digital transformation: Cybersecurity law plays an important role in creating the legal foundation for a safe, transparent, and sustainable digital transformation process.

2.2.4. Theoretical structure of cybersecurity law

The theoretical structure of cybersecurity law comprises six institutional groups, including: regulations on principles of cybersecurity protection; regulations on acts violating cybersecurity law; regulations on sanctions against violating acts; regulations on the legal status of subjects; regulations on measures for cybersecurity protection; regulations on international cooperation in the field of cybersecurity. This constitutes the theoretical structure to identify the content of cybersecurity law, and simultaneously serves as the basis for evaluating the current status and proposing solutions to improve the law in the subsequent sections of the thesis.

2.3. CONCEPT AND CRITERIA FOR IMPROVING THE LAW ON CYBERSECURITY IN VIETNAM

2.3.1. Concept of improving cybersecurity law

Improving cybersecurity law is the process of reviewing, evaluating, amending, supplementing, repealing, or promulgating new legal norms on cybersecurity, while consolidating the enforcement mechanism, safeguarding institutions, resources, technical standards, coordination mechanisms, and mechanisms for controlling the application of the law, aiming to build a complete, synchronous, transparent, feasible legal system that adapts to technological development, ensuring the effectiveness of protecting national security and social order and safety, whilst protecting the legitimate rights and interests of individuals and organizations in cyberspace.

2.3.2. Criteria for evaluating the perfection of cybersecurity law

First, the group of criteria regarding legal content, including completeness, synchronicity, adaptability to technology, and the level of ensuring the legitimate rights and interests of individuals and organizations.

Second, the group of criteria regarding legislative techniques, including transparency and legislative techniques.

Third, the group of criteria regarding law enforcement, including feasibility and the effectiveness of the enforcement mechanism.

2.4. CONDITIONS ASSURING THE IMPROVEMENT OF CYBERSECURITY LAW

2.4.1. Political - legal conditions: First and foremost, improving cybersecurity law must ensure conformity with the Constitution. Legal regulations on cybersecurity must ensure consistency with constitutional principles on defending the Fatherland, protecting national security, ensuring social order and safety, respecting, protecting, and guaranteeing human rights and civil rights; aligned with the Party's viewpoints and guidelines on scientific development, technology, innovation, and national digital transformation.

2.4.2. Conditions regarding theoretical awareness and legislative thinking: Primarily, cybersecurity law needs to be constructed based on a correct awareness of the interdisciplinary nature of this field.

2.4.3. Conditions regarding institutions and coordination mechanisms: First, there is a need for sufficiently robust enforcement institutions with clearly defined functions, tasks, and authorities; a unified, regular, and mandatory inter-agency coordination mechanism must be established, coupled with an accountability control mechanism.

2.4.4. Conditions regarding human and technical resources: Initially, a contingent of legal experts knowledgeable in cybersecurity is required. Beyond the human element, cybersecurity law also demands appropriate technical infrastructure.

2.4.5. Conditions regarding international cooperation: Primarily, improving cybersecurity law needs to be linked with international cooperation on information sharing and threat warning.

2.4.6. Conditions regarding supervision, accountability, and the protection of human rights and civil rights in cyberspace: The condition regarding supervision, accountability, and rights protection is a crucial condition ensuring that the process of improving cybersecurity law is carried out consistently with the requirements of a rule-of-law State.

2.5. CYBERSECURITY LAW OF SELECTED COUNTRIES, INTERNATIONAL ORGANIZATIONS, AND REGIONS WORLDWIDE, AND REFERENCE VALUES FOR VIETNAM

2.5.1. Cybersecurity law of selected countries, international organizations, and regions worldwide

The thesis selects the United States, the European Union, the Russian Federation, China, and Singapore as objects for comparative research based on their representation of different approaches to cybersecurity law models globally.

2.5.2. Several lessons learned for Vietnam

Identify cybersecurity as a critical content of national security protection, social order and safety, and digital economy development.

Mandate the use of real information when utilizing services in cyberspace; strictly prohibit the spread of fake news on social networks.

Openly monitor, block, and filter distorted, untruthful information in cyberspace.

Develop a set of rules, standards, and technical regulations in the field of cybersecurity.

Design penalty sanctions in a tiered manner, proportionate to the nature, extent, consequences, and scale of the violation.

Chapter 3

THE REALITY OF THE LAW AND THE PRACTICAL ENFORCEMENT OF CYBERSECURITY LAW IN VIETNAM TODAY

3.1. THE FORMATION AND DEVELOPMENT PROCESS OF THE LAW ON CYBERSECURITY IN VIETNAM

The thesis evaluates the formation and development process of the law on cybersecurity in Vietnam based on six basic legal institutions across different periods: before 2013, from 2013 to prior to the promulgation of the 2018 Cybersecurity Law, and after the promulgation of the 2018 Cybersecurity Law to the present.

3.2. EVALUATION OF THE CURRENT LAW ON CYBERSECURITY IN VIETNAM

3.2.1. Strengths and causes of strengths of the law on cybersecurity in Vietnam

3.2.1.1. Strengths of the law on cybersecurity in Vietnam

- Strengths in the provisions on cybersecurity protection principles

First, based on the criteria group regarding legal content, the provisions on cybersecurity protection principles have initially ensured comprehensiveness, synchronization, adaptability to technology, and the requirements for protecting the legitimate rights and interests of entities in cyberspace. Second, based on the criteria group regarding legislative

technique, cybersecurity protection principles are directly stipulated in the 2018 Cybersecurity Law with relatively generalized, stable, and highly directional content. Third, based on the criteria group regarding law enforcement, cybersecurity protection principles have created a legal basis for determining responsibilities and coordination mechanisms among entities participating in cybersecurity protection.

- Strengths in the provisions on acts violating the law on cybersecurity

First, based on the criteria group regarding legal content, the current law has gradually and relatively comprehensively identified the basic groups of violations in cyberspace. Second, based on the criteria group regarding legislative technique, acts violating cybersecurity laws have gradually been described more specifically and clearly. Third, based on the criteria group regarding law enforcement, the relatively clear identification of violation groups by the law has created an important basis for preventing, detecting, stopping, and handling acts that infringe upon cybersecurity.

- Strengths in the provisions on handling sanctions for acts violating the law on cybersecurity

First, based on the criteria group regarding legal content, the current law has initially established a relatively diverse system of sanctions, appropriate to the nature and danger level of the violations. Second, based on the criteria group regarding legislative technique, the provisions on sanctions have initially been designed more clearly in terms of handling forms, handling levels, authority to apply, and legal consequences. Third, based on the criteria group regarding law enforcement, the provisions on sanctions have created an important legal basis for the prevention, detection, stopping, handling, and remediation of consequences of cybersecurity infringements.

- Strengths in the provisions on the legal status of entities participating in cybersecurity activities

First, based on the criteria group regarding legal content, the law on cybersecurity has gradually established a relatively complete set of entity groups participating in cybersecurity protection. Second, based on the criteria group regarding legislative technique, the law has gradually clarified the rights, obligations, responsibilities, and authority of each entity group. Third,

based on the criteria group regarding law enforcement, these provisions have created a basis for multi-entity coordination mechanisms in cybersecurity protection.

- Strengths in the provisions on cybersecurity protection measures

First, based on the criteria group regarding legal content, the law on cybersecurity has initially established a relatively comprehensive system of protection measures, covering multiple stages of the cybersecurity protection process. Second, based on the criteria group regarding legislative technique, cybersecurity protection measures have been categorized into relatively clear groups with different names, purposes, and scopes of application. Third, based on the criteria group regarding law enforcement, the provisions on cybersecurity protection measures have created a legal basis for organizing the implementation of cybersecurity protection tasks in practice.

- Strengths in the provisions on international cooperation in cybersecurity

First, based on the criteria group regarding legal content, the law on cybersecurity has initially acknowledged the content of international cooperation relatively fully. Second, based on the criteria group regarding legislative technique, the law has initially established the principles, contents, and responsibilities for international cooperation in the field of cybersecurity in a relatively clear direction. Third, based on the criteria group regarding law enforcement, the provisions on international cooperation have created a legal basis for improving the capacity to prevent, detect, investigate, handle, and remediate the consequences of cybersecurity infringements with foreign elements.

3.2.1.2. Causes of the strengths in the law on cybersecurity in Vietnam

The strengths of the law on cybersecurity in Vietnam did not emerge spontaneously but are the result of the process of awareness, policy formulation, institutional improvement, and enforcement organization across multiple stages.

3.2.2. Shortcomings, inadequacies, and causes of shortcomings and inadequacies of the law on cybersecurity in Vietnam

3.2.2.1. Shortcomings and inadequacies of the law on cybersecurity in Vietnam

- Shortcomings and inadequacies in the provisions on cybersecurity protection principles

First, based on the criteria group regarding legal content, the current system of cybersecurity protection principles does not fully cover the specific requirements of cybersecurity governance in the context of digital transformation. Second, based on the criteria group regarding legislative technique, some cybersecurity protection principles still lack transparency and do not ensure the necessary level of clarity for uniform application. Third, based on the criteria group regarding law enforcement, the translation of cybersecurity protection principles into specific implementation mechanisms is not yet synchronized and truly feasible.

- Shortcomings and inadequacies in the provisions on acts violating the law on cybersecurity

First, based on the criteria group regarding legal content, the current law does not fully cover newly emerging violations in cyberspace. Second, based on the criteria group regarding legislative technique, some provisions on acts violating cybersecurity laws lack specific identification criteria, leading to difficulties in uniform application. Third, based on the criteria group regarding law enforcement, identifying, classifying, and evaluating the danger level of acts violating cybersecurity laws still face many difficulties in practice.

- Shortcomings and inadequacies in the provisions on cybersecurity protection measures

First, based on the criteria group regarding legal content, the current cybersecurity protection measures do not fully cover newly emerging risks and threats in cyberspace. Second, based on the criteria group regarding legislative technique, some cybersecurity protection measures are not clearly defined regarding conditions, scope, sequences, procedures, and application limits. Third, based on the criteria group regarding law enforcement, the application of cybersecurity protection measures still faces difficulties due to limitations in resources, manpower, technical tools, and coordination mechanisms.

- Shortcomings and inadequacies in the provisions on the legal status of entities participating in cybersecurity activities

First, based on the criteria group regarding legal content, the current law has not fully and adequately determined the legal status of new entities in the digital ecosystem. Second, based on the criteria group regarding legislative technique, some provisions on the rights, obligations, and responsibilities of entities are still overly general. Third, based on the criteria group regarding law enforcement, the coordination mechanism among entities is still fragmented, overlapping, or lacking a unified coordinating focal point.

- Shortcomings and inadequacies in the provisions on handling sanctions for acts violating the law on cybersecurity

First, based on the criteria group regarding legal content, the current sanction system does not fully cover new types of violations and new violating entities in the digital environment. Second, based on the criteria group regarding legislative technique, some provisions on sanctions lack clarity in distinguishing between forms of penalties, remedial measures, and state management measures. Third, based on the criteria group regarding law enforcement, the application of sanctions in practice still faces many difficulties, especially concerning commercial legal entities, cross-border platforms, and entities deriving massive illicit profits from violations in cyberspace.

- Shortcomings and inadequacies in the provisions on international cooperation in cybersecurity

First, based on the criteria group regarding legal content, the provisions on international cooperation in the cybersecurity field do not fully cover the necessary cooperation mechanisms. Second, based on the criteria group regarding legislative technique, the current law still lacks detailed provisions on the collection, preservation, transfer, and use of cross-border electronic evidence. Third, based on the criteria group regarding law enforcement, international cooperation in the cybersecurity field still faces difficulties due to differences in jurisdiction, evidentiary standards, procedural sequences, enforcement capacity, and the level of cooperation readiness among countries.

3.2.2.2. Causes of the shortcomings and limitations in the law on cybersecurity in Vietnam

The shortcomings and inadequacies of the law on cybersecurity in Vietnam stem from various causes, including both objective and subjective ones. These causes have an interactive relationship with each other, reflecting the characteristics of cybersecurity as a new field that is highly technical, interdisciplinary, cross-border, and constantly changing rapidly alongside technological developments.

3.3. EVALUATING THE PRACTICAL ENFORCEMENT OF CYBERSECURITY LAW IN VIETNAM TODAY

3.3.1. The practice of complying with cybersecurity law: The practical implementation of cybersecurity law in the 2019-2025 period shows that the awareness of legal compliance among agencies, organizations, enterprises, and individuals has experienced positive changes. Besides the achieved results, the practical compliance with cybersecurity law still presents many limitations. The situation of cyberattacks, cyber espionage, exposure and loss of state secrets, illegal data collection and trading, online fraud, and the dissemination of fake news and malicious information remains complex.

3.3.2. The practice of executing cybersecurity law: Recently, the institutionalization, promulgation, and organization of implementing mechanisms, policies, schemes, and projects related to cybersecurity have been deployed relatively synchronously. The system of normative legal documents on cybersecurity, personal data protection, telecommunications, Internet management, and network information security has gradually been constructed and perfected, creating a legal corridor for agencies, organizations, enterprises, and individuals to deploy activities ensuring information security and cybersecurity. However, the execution of cybersecurity law still possesses certain limitations.

3.3.3. The practice of utilizing cybersecurity law: Recent practice shows that state agencies, organizations, enterprises, and individuals have progressively utilized legal regulations, tools, and mechanisms on cybersecurity to protect information systems, data, and their legitimate rights and interests in cyberspace. However, the practical utilization of cybersecurity law still presents certain limitations.

3.3.4. The practice of applying cybersecurity law: The practical application of cybersecurity law recently has achieved many distinct results,

most notably in combating and handling crimes and law-violating acts in cyberspace. Besides the achieved results, the application of cybersecurity law still possesses certain limitations. Some regulations remain overlapping among domains of cybersecurity, network information security, personal data protection, telecommunications, encryption, and the management of cross-border platforms, leading to difficulties in determining jurisdiction, sequences, procedures, and presiding responsibilities when handling specific cases. Many incidents simultaneously involve personal data, bank accounts, e-wallets, telecommunication subscribers, IP addresses, cross-border platforms, e-commerce, and high-tech crimes, requiring tight inter-agency coordination; however, current legal mechanisms and coordination processes are not truly synchronous.

3.3.5. General remarks on the practical implementation of the law on cybersecurity in Vietnam. The practical implementation of the law on cybersecurity still exhibits numerous limitations across all four dimensions: legal compliance, execution, utilization, and application. Prominent issues include sophisticated cybercrime, uncoordinated inter-sectoral collaboration, and ambiguities in handling cross-border cases. These limitations stem from the borderless nature of cyberspace (objective factors) alongside subjective bottlenecks in capacity, technical infrastructure, and compliance awareness. Such shortcomings in the implementation stage represent the primary barrier obstructing the effectiveness of the law. This serves as an essential practical foundation for the thesis to propose solution groups aimed at enhancing enforcement efficiency in Chapter 4.

Chapter 4

REQUIREMENTS, VIEWPOINTS, AND SOLUTIONS FOR IMPROVING THE LAW ON CYBERSECURITY IN VIETNAM

4.1. REQUIREMENTS FOR IMPROVING THE LAW ON CYBERSECURITY IN VIETNAM

Ensure the comprehensive, direct leadership of the Party, highly promoting the Party nature in improving cybersecurity law.

Innovate thinking, directing the improvement of cybersecurity law to simultaneously ensure state management requirements and encourage innovation and creativity.

Create breakthroughs, tightly linking the formulation and improvement of cybersecurity law with law execution in reality.

Enhance digital transformation, application of artificial intelligence, and big data in the task of improving cybersecurity law.

4.2. VIEWPOINTS ON IMPROVING THE LAW ON CYBERSECURITY IN VIETNAM

Improving cybersecurity law must ensure a balance between protecting national security and protecting the legitimate rights and interests of individuals and organizations.

Improving cybersecurity law must be based on risk governance, not solely on post-violation handling.

Improving cybersecurity law must ensure synchronicity between legal norms and enforcement mechanisms.

Improving cybersecurity law must adapt to technology but not chase after every single technical phenomenon.

4.3. SOLUTIONS FOR IMPROVING THE LAW ON CYBERSECURITY IN VIETNAM

4.3.1. Solution group for improving cybersecurity legal content according to institutional groups

4.3.1.1. Improving the group of regulations on cybersecurity protection principles: First, supplement the cybersecurity risk governance principle. Second, specify and clarify the principle of balancing national security protection requirements with ensuring the legitimate rights and interests of individuals and organizations in documents guiding the implementation of

cybersecurity law. Third, supplement the principle of accountability in cybersecurity protection activities. Fourth, supplement the principle of multi-subject coordination in cybersecurity protection.

4.3.1.2. Improving the group of regulations on acts violating cybersecurity law: First, redesign regulations on acts violating cybersecurity law according to a model combining the listing of typical acts and open identification criteria. Second, supplement or specify newly emerging groups of violating acts in cyberspace. Third, clarify the boundary between administrative law violations and criminal offenses in the field of cybersecurity. Fourth, supplement and improve regulations on electronic evidence and damage quantification in handling acts violating cybersecurity law.

4.3.1.3. Improving the group of regulations on sanctions against acts violating cybersecurity law: First, it is necessary to tier handling sanctions according to the level of risk, consequence, and dangerous nature of the violating act. Second, it is necessary to strengthen sanctions aimed at consequence rectification and the restoration of legitimate rights and interests of infringed subjects. Third, it is necessary to improve sanctions for organizations and enterprises providing services in cyberspace. Fourth, it is necessary to ensure that handling sanctions do not generate an unreasonable compliance burden for individuals, organizations, and enterprises. Fifth, it is necessary to ensure consistency among administrative sanctions, criminal sanctions, civil liability, and consequence rectification measures.

4.3.1.4. Improving the group of regulations on the legal status of subjects operating in the cybersecurity field: First, clearly demarcate authority among state agencies in the cybersecurity field. Second, improve the legal status of the specialized cybersecurity protection force. Third, supplement and clarify the legal responsibilities of enterprises providing services in cyberspace. Fourth, supplement and specify the rights of individuals and organizations in cyberspace. Fifth, improve coordination mechanisms between the State, enterprises, and users in cybersecurity protection.

4.3.1.5. Improving the group of regulations on cybersecurity protection measures: First, design cybersecurity protection measures along the risk

governance chain. Second, clearly regulate the conditions for applying intervention measures into information systems, data, and activities in cyberspace. Third, supplement the principle of proportionality in applying cybersecurity protection measures. Fourth, supplement and improve supervision, complaint, and accountability mechanisms in applying cybersecurity protection measures. Fifth, improve technical standards, regulations, and professional processes in cybersecurity protection. Sixth, improve coordination mechanisms among state agencies, enterprises, and information system administrators in applying cybersecurity protection measures.

4.3.1.6. Improving the group of regulations on international cooperation in cybersecurity: First, research and improve regulations on the collection, preservation, and cross-border transfer of electronic evidence. Second, supplement and improve cooperation mechanisms with cross-border service providers. Third, supplement and expand international cooperation in warning, information sharing, and cybersecurity incident response.

4.3.2. Solution group for ensuring synchronicity, transparency, and legislative quality in the cybersecurity field

4.3.2.1. Review, systematization, and resolution of overlaps among legal documents: Foremost, it is necessary to organize a comprehensive review of regulations related to cybersecurity within the current legal system. Additionally, unified review criteria must be developed to ensure the review results possess practical value.

4.3.2.2. Enhancing the quality of policy impact assessment: Enhancing the quality of policy impact assessment is a critical solution. To enhance the quality of policy impact assessment, it must be ensured that the assessment is based on evidence, data, and substantive consultation.

4.3.2.3. Standardizing terminology and legislative techniques: A unified legal terminology system in the field of cybersecurity must be developed. Concurrently, mechanisms for explaining and guiding the application of legal-technical terminology in the cybersecurity field must be established.

4.3.3. Solution group in organizing the implementation of cybersecurity law

4.3.3.1. Enhancing the capacity of cybersecurity law enforcement agencies: First, specialized training for the cybersecurity law enforcement

personnel must be enhanced. Simultaneously, cybersecurity law enforcement capacity at the local level must be improved, not solely concentrated at the central level. Furthermore, coordination mechanisms among law enforcement agencies in the cybersecurity field must be improved. Alongside the human factor, technical tools for detecting, warning, monitoring, investigating, and responding to cybersecurity incidents must be invested in.

4.3.3.2. Establishing clear inter-agency coordination mechanisms: Accordingly, the presiding agency and coordinating agencies must be clearly identified in each specific group of activities. Inter-agency coordination mechanisms must specify handling time limits for each type of case.

4.3.3.3. Ensuring resources for law execution: Foremost, stable budget resources must be ensured, appropriate to cybersecurity protection requirements in each phase. Alongside budget resources, emphasis must be placed on developing high-quality human resources in the cybersecurity field. Furthermore, technical infrastructure and technological tools must be ensured to serve the execution of cybersecurity law. Investment in technical infrastructure must be targeted and focused, avoiding scattered, formalistic investments or those unsuited to actual operational capacity.

CONCLUSION

In the context of national digital transformation, cyberspace has become an important environment for the operations of the State, the economy, and social life. Along with the benefits brought by digital technology, the threats infringing upon cybersecurity are increasingly escalating in scale, nature, complexity, and consequences. Cybersecurity is therefore no longer a purely technical issue, but has become a political-legal issue, directly linked to protecting national security, social order and safety, national sovereignty in cyberspace, human rights, civil rights, and the sustainable development of the country. Therefore, improving the law on cybersecurity in Vietnam is an objective, urgent requirement of strategic significance.

The thesis has established a criteria system for evaluating the degree of perfection of cybersecurity law in Vietnam, comprising three groups: the criteria group on legal content, including completeness, synchronicity, adaptability to technology, and the level of ensuring the legitimate rights and interests of individuals and organizations; the criteria group on legislative techniques, including transparency and legislative techniques; the criteria group on law enforcement, including feasibility and the effectiveness of the enforcement mechanism. Regarding the current status, the thesis shows that cybersecurity law in Vietnam has gradually formed and developed from dispersed regulations within the laws on information technology, telecommunications, electronic transactions, network information security, and violation handling to a specialized phase with the 2018 Law on Cybersecurity and implementing guidelines. The National Assembly's passage of the Law on Cybersecurity No. 116/2025/QH15 continues to demonstrate the trend of improving the law towards uniformity, synchronicity, and better alignment with the requirements of cyberspace governance in the digital transformation context. However, cybersecurity law in Vietnam still harbors certain limitations and inadequacies. Based on this, the thesis proposes solution groups to improve cybersecurity law in terms of legal content and enforcement organization.

LIST OF AUTHOR'S PUBLISHED WORKS RELATED TO THE THESIS TOPIC

1. Bui Thi Thuy Dung (2022), Monograph *Traditional Security and Non-Traditional Security in the context of the Fourth Industrial Revolution*, People's Public Security Publishing House, Hanoi.

2. Bui Thi Thuy Dung (2023), The value of the work “Cyberspace Sovereignty - The Imperative of the Era and National Obligation” to the process of improving cybersecurity law, *Proceedings of the Scientific Conference “Scientific Commentary on the book “Cyberspace Sovereignty - The Imperative of the Era and National Obligation”*, Hanoi.

3. Bui Thi Thuy Dung (2025), Recommendations for improving criminal law on cybersecurity in Vietnam today, *State Management Review*, issue 352 (May 2025), Hanoi.

4. Bui Thi Thuy Dung, Trieu Manh Tung (2025), Innovating legal thinking on cybersecurity in the new era, *Communist Review*, Hanoi.

5. Bui Thi Thuy Dung (2025), International experience in cryptocurrency management and suggestions for Vietnam, *State Management Review*, issue August 2025, Hanoi.

6. Bui Thi Thuy Dung (2025), Identifying plots to transform social order and safety issues into national security issues by hostile forces today, *People's Public Security Review*, issue March 2025, Hanoi.

7. Bui Thi Thuy Dung (2025), Plots and activities of abusing religion to transform social order and safety issues into national security issues in cyberspace today, *People's Public Security Political Theory Review*, issue October 2025, Hanoi.