BILINGUAL PUBLISHING GROUP

Journal of Computer Science Research

https://journals.bilpubgroup.com/index.php/jcsr

REVIEW

Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implication

Runhua Tang [1], ***Wenyi Zhang*** [2*]

[1] *School of Journalism and Communication, Dalian University of Foreign Languages, Dalian 116044, China*

[2] *School of Information Management, Nanjing University, Nanjing 210000, China*

ABSTRACT

This review critically examines Li Zhi's Legal Comparisons and Implications of Cyberspace Security Governance, situating it within ongoing scholarly debates on international law, comparative jurisprudence, and the multidimensional challenges of global cybersecurity. By providing a nuanced textual and comparative analysis of major legal frameworks—ranging from the Tallinn Manual 2.0 to national statutes in the United States, the European Union, and Asia—Li's work contributes significantly to clarifying conceptual boundaries between network security and cyberspace security. Drawing on authoritative comparative law studies and incorporating insights from multi-stakeholder governance research, this review highlights the book's core theoretical contributions, its critical appraisal of divergent international governance models, and the practical implications of its policy recommendations. Although the volume effectively outlines current governance challenges and norms, it also opens new avenues for future inquiry into rapidly evolving technologies and their legal ramifications. In doing so, this review not only underscores Li's methodological rigor and integrative approach but also encourages further scholarship to refine and adapt the global legal order for a more secure and equitable cyberspace.

Keywords: Cyberspace Security; International Law; Comparative Legal Analysis; Multi-Stakeholder Governance; Cross-Jurisdictional Cooperation

*CORRESPONDING AUTHOR:

Wenyi Zhang, School of Information Management, Nanjing University, Nanjing 210000, China; Email: 602024140037@smail.nju.edu.cn

ARTICLE INFO

Received: 24 January 2025 | Revised: 4 February 2025 | Accepted: 5 February 2025 | Published Online: 10 February 2025
DOI: https://doi.org/10.30564/jcsr.v7i1.8555

CITATION

Tang, R., Zhang, W., 2025. Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implication. Journal of Computer Science Research. 7(1): 1–10. DOI: https://doi.org/10.30564/jcsr.v7i1.8555

1. Introduction

The rapid development and deep integration of the Internet into political, economic, and social spheres have intensified the complexity and urgency of cyberspace security governance at both national and international levels. As cyberspace transcends traditional territorial boundaries and eludes conventional notions of sovereignty, established international legal frameworks and governance models struggle to address challenges posed by state and non-state cyber operations [1, 2]. High-profile cyber incidents such as the 2015 Office of Personnel Management (OPM) breach in the United States, the 2020 SolarWinds attack, and recurrent large-scale ransomware campaigns underscore the vulnerability of critical infrastructures, highlighting gaps in prevailing norms and enforcement mechanisms [3, 4]. Meanwhile, the adoption of sweeping regulatory measures like the European Union's Directive on Security of Network and Information Systems (NIS Directive) and the Cybersecurity Law of the People's Republic of China reflects a growing international recognition of the need to bolster legal and policy regimes [5].

Against this backdrop, Li Zhi's Legal Comparisons and Implications of Cyberspace Security Governance offers a timely and comprehensive examination of legal texts, policy measures, and governance practices implemented by various states and international organizations. By weaving together insights from international law, comparative jurisprudence, and empirical case studies, Li's monograph provides valuable analytical tools to understand the evolving transnational landscape of cyber norm development and enforcement. This review critically assesses the book's contributions through an Introduction, followed by a Literature Review that situates the study within broader theoretical debates. The Research Methods section evaluates the empirical rigor and theoretical foundations of the author's approach, while the Comparative Analysis synthesizes key insights drawn from multiple jurisdictions and institutional frameworks. Finally, the Conclusion discusses the work's theoretical implications, policy relevance, and avenues for future scholarship. Throughout, this review integrates authoritative academic literature and empirical evidence to elucidate the strengths, limitations, and continuing significance of Li's analysis in shaping a more resilient global cyberspace governance architecture.

2. Literature Review

Existing research on cybersecurity governance reveals complex challenges arising from the transnational and often elusive nature of cyber threats, including the ambiguity of international legal frameworks, divergent national policies, and asymmetric distributions of power and resources among stakeholders [2, 4]. Within the broader domain of cybersecurity studies, scholars have emphasized the global proliferation of cyber incidents and the strategic manipulation of digital infrastructures, highlighting the need for robust theoretical models to understand state and non-state cyber operations [3, 6]. Moreover, policy-oriented literature has illustrated that effective cyber deterrence, resilience-building, and norm development require not only improved technical countermeasures but also nuanced diplomatic engagement and confidence-building measures [1].

Turning specifically to the legal dimension, research on cybersecurity law has critically examined the adequacy of existing treaties, customary international law, and emerging soft-law instruments. The *Tallinn Manual 2.0* stands as a benchmark for delineating how traditional international law might apply to cyber warfare, yet its enforceability and normative clarity remain subject to debate, reflecting a broader tension between evolving cyber threats and relatively static legal principles [7]. Empirical analyses of national cybersecurity legislations—such as the European Union's regulatory approach or the United States' emphasis on national security—demonstrate how political, economic, and cultural factors shape differing governance models, thus reinforcing the importance of comparative legal studies to identify best practices and harmonize international standards [8, 9].

From a methodological standpoint, scholarship on legal research techniques provides critical insights into how diverse jurisdictions interpret and operationalize legal norms in the cyber domain. Comparative legal methodology not only elucidates social values and institutional logics underlying varied normative arrangements [10], but also assists scholars in evaluating the internal coherence, applicability, and cultural adaptability of cyber law [11]. In this vein, combining doctrinal analysis, comparative jurisprudence, and empirical inquiry can reveal both the universal principles that might guide global governance and the context-specific nuances that inform policy implementation [12].

By integrating these three strands, namely general cy-

bersecurity research, cybersecurity law scholarship, and legal research methods, studies can better capture the multidimensional challenges of cyberspace governance and move forward toward a more coherent, inclusive, and enforceable international legal framework. This integration enables a more comprehensive understanding of the complex issues at play and paves the way for the development of a more robust and effective legal regime for cyberspace. It also highlights the importance of interdisciplinary research in addressing the complex challenges of cyberspace governance and the need for a collaborative approach among scholars and practitioners from different fields.

3. Research Methods

3.1. A Review of the Research Methods of This Book

In the book *Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implications*, Professor Li Zhi adopts a comprehensive research method for analysis, and the method is highly innovative.

(1) Data collection and processing

In order to significantly enhance the empirical validity and contextual relevance, the author meticulously employs the advanced method of data mining. With the powerful tool of Python programs, the author precisely captures a vast amount of information. This information mainly comes from multiple important fields, including the field of academic research, which encompasses the in-depth research findings and cutting-edge viewpoints of many experts and scholars; the field of policy reports, which includes the formulation and implementation of network security policies by government departments and related analyses and suggestions; and the media field, which involves detailed reports by the media on network security incidents and their extensive impacts. Through this comprehensive and systematic capturing method, the author obtains a large amount of valuable qualitative data.

(2) Textual Analysis

The author conducts in-depth and exhaustive textual examinations of international treaties, policy documents, and national laws, with the overarching aim of precisely defining the legal implications, underlying intentions, and key focal points of these legal instruments. For instance, in the comprehensive analysis of the Tallinn Manual 2.0, not only is the meticulous delineation of cyber conflicts and the comprehensive assessment of the applicability of legal principles provided, but also its limitations in actual international legal practice are critically evaluated by employing advanced legal theories and methodologies.

(3) Comparative Study

Leveraging the comparative legal methodology, the author situates the cybersecurity governance strategies of the United States, the European Union, Russia, Japan, Singapore, and India within a singular analytical framework. Through a meticulous comparison of legislation priorities, enforcement mechanisms, approaches to international cooperation, and technological investments, the study astutely identifies both the strengths and weaknesses of various governance models, furnishing empirical underpinnings for formulating more adaptive and inclusive global norms.

In sum, the integration of textual analysis, comparative research, and qualitative data interpretation not only crystallizes the norms but also validates the empirical aspects, endowing the study with an outstanding methodological soundness.

3.2. The Research Method Adopted in This Paper

On the one hand, textual analysis was employed to conduct an overall study on this book. Firstly, attention was paid to the definitions, concepts, theoretical frameworks and so on in the text to understand how the author defined and explained the core concepts regarding cyberspace security governance. Secondly, the argumentation methods, logical structures as well as the cited cases and data used by the author were noted, and an analysis was made on how they supported or elaborated on the viewpoints.

Based on the thorough close reading results, the text was precisely coded using Nvivo12 qualitative analysis software, an indispensable tool. This allowed for the effective identification and orderly organization of core and subthemes into three comprehensive coding tiers. The coding process not only grouped related ideas but also enabled a more systematic and detailed analysis. Categorizing the text into these tiers made it possible to explore the underlying patterns and relationships, providing valuable insights and a deeper understanding of the subject.

First-Level Coding: In this initial stage, the analysis focuses on extracting primary themes or overarching topics evident throughout the text. These may include broad categories such as "Network Space and Governance Basics," "Governance Actors and Responsibilities," "Governance Tools and Mechanisms," "Governance Challenges and Responses," and "Governance Outcomes and Evaluation."

Second-Level Coding: Following the establishment of main themes, each first-level code is further refined into sub-themes or dimensions that illuminate the various facets of the overarching topic. For example, under the "Network Space and Governance Basics" theme, sub-codes such as "Conceptual Foundation" and "Conceptual Framework" can be introduced. These second-level codes serve to decompose the primary themes into more precise, manageable units of analysis.

Third-Level Coding: At this level, the analysis delves deeper into the sub-themes by identifying specific concepts and statements. This involves isolating key phrases, sentences, or paragraphs that reflect distinct ideas within each sub-theme. Third-level codes are then assigned to these finer-grained elements, allowing for a more detailed examination. For instance, under the "Threats and Risks" sub-theme, one might develop codes like "Government Policies and Strategies" and "Agency Roles and Responsibilities" to capture and label these particular dimensions of the content. Full details are provided in **Table 1**.

Table 1. Three-Level Coding Framework for Book Text Analysis.

Level 1	Level 2	Level 3	Description
Network Space and Governance Basics	Conceptual Foundation	Definition and Characteristics	Defines the concept of cyberspace, including its nature, scope, and unique features. Explores how cyberspace differs from traditional physical spaces and the implications for governance.
		Key Attributes	Identifies and analyzes the key attributes of cyberspace, such as its virtuality, connectivity, and anonymity. Examines how these attributes affect the governance of cyberspace and the challenges it poses.
	Conceptual Framework	Legal and Policy Frameworks	Reviews the legal and policy frameworks that govern cyberspace, including international treaties, national laws, and regional regulations. Analyzes the role of these frameworks in shaping the governance of cyberspace and ensuring security.
Governance Actors and Responsibilities	National Governance	Government Policies and Strategies	Examines the policies and strategies adopted by national governments to manage cyberspace security. This includes measures such as legislation, regulatory frameworks, and investment in cybersecurity capabilities.
		Agency Roles and Responsibilities	Defines the roles and responsibilities of various national agencies involved in cyberspace security governance, such as the intelligence agencies, law enforcement agencies, and regulatory bodies. Analyzes how these agencies collaborate and coordinate to address cyber threats.
	International Organizations	United Nations Initiatives	Explores the role of the United Nations in global cyberspace security governance. This includes initiatives such as the development of international norms and standards, and the promotion of international cooperation in cybersecurity.
		Regional Alliances and Cooperation	Analyzes the role of regional alliances, such as the European Union and the Asia-Pacific Economic Cooperation (APEC), in promoting regional cooperation in cyberspace security. Examines the development of regional frameworks and initiatives for cybersecurity.

Table 1. *Cont.*

Level 1	Level 2	Level 3	Description
Governance Tools and Mechanisms	Legal Instruments	Laws and Regulations	Reviews the relevant laws and regulations governing cyberspace security at the national and international levels. This includes laws related to cybercrime, data protection, and network security. Analyzes the effectiveness of these laws in addressing cyber threats and protecting the rights and interests of individuals and organizations.
		International Treaties	Europe's Convention on Cybercrime and the United Nations Convention on the Use of Electronic Communications in International Contracts. Analyzes the significance of these treaties in promoting international cooperation and establishing common norms for cybersecurity.
	Technical Measures	Cybersecurity Technologies	Evaluates the various cybersecurity technologies used to protect cyberspace, such as firewalls, intrusion detection systems, and encryption technologies. Analyzes the effectiveness of these technologies in preventing cyber attacks and protecting sensitive information.
		Data Protection and Privacy Tools	Assesses the data protection and privacy tools used in cyberspace, such as data encryption, access controls, and data minimization principles. Analyzes the importance of these tools in ensuring the privacy and security of personal data in the digital age.
Governance Challenges and Responses	Threats and Risks	Cyber Attacks	Identifies and analyzes the various types of cyber attacks, such as malware attacks, phishing attacks, and distributed denial-of-service (DDoS) attacks. Examines the impact of these attacks on individuals, organizations, and national security.
		Data Breaches	Explores the issue of data breaches and the potential consequences for individuals and organizations. Analyzes the causes of data breaches, such as human error, system vulnerabilities, and external attacks. Examines the measures taken to prevent and respond to data breaches, such as data backup and recovery, and incident response planning.
		Cybercrime	Evaluates the prevalence and impact of cybercrime in cyberspace, such as online fraud, identity theft, and child pornography. Analyzes the legal and enforcement challenges in combating cybercrime and the role of international cooperation in addressing these challenges.
	Responses and Mitigation	Policy Responses	Examines the policy responses adopted by governments and international organizations to address cyberspace security challenges. This includes the development of national cybersecurity strategies, the establishment of international cooperation mechanisms, and the promotion of public-private partnerships in cybersecurity.
		Technical Responses	Assesses the technical responses used to address cyber threats, such as the development of new cybersecurity technologies, the improvement of network security infrastructure, and the implementation of threat intelligence systems. Analyzes the role of technology in enhancing cyber resilience and preventing cyber attacks.

Table 1. *Cont.*

Level 1	Level 2	Level 3	Description
Governance Outcomes and Evaluation	Effectiveness and Impact	Security Outcomes	Evaluates the effectiveness of cyberspace security governance in achieving its intended outcomes, such as the protection of national security, the prevention of cyber attacks, and the protection of personal data. Analyzes the key performance indicators (KPIs) used to measure security outcomes and the challenges in collecting and analyzing these indicators.
		Stakeholder Engagement	Assesses the level of stakeholder engagement in cyberspace security governance, including government agencies, the private sector, civil society organizations, and individuals. Analyzes the role of stakeholder engagement in shaping the governance agenda, promoting cooperation, and ensuring the accountability of governance actors.
	Emerging Trends	Technological Advancements	Monitors the emerging technological advancements in cyberspace, such as artificial intelligence, blockchain technology, and the Internet of Things (IoT). Analyzes the potential impact of these advancements on cyberspace security and the governance challenges they pose.
		Globalization and International Cooperation	Explores the trends towards globalization and international cooperation in cyberspace security governance. Analyzes the role of international organizations, regional alliances, and multilateral cooperation mechanisms in addressing global cyber challenges and promoting international security.
		Social and Cultural Changes	Examines the social and cultural changes that are occurring in the digital age and their impact on cyberspace security governance. This includes issues such as digital literacy, online activism, and the role of social media in shaping public opinion and social behavior.

The presented three-level coding framework provides a structured approach to analyzing the book's content by progressively refining the categorization from broad thematic areas to increasingly specific concepts. At the first level, overarching themes such as "Network Space and Governance Basics," "Governance Actors and Responsibilities," "Governance Tools and Mechanisms," "Governance Challenges and Responses," and "Governance Outcomes and Evaluation" establish the primary domains of inquiry. Within these domains, second-level coding delineates key sub-themes that clarify the core ideas and dimensions underlying each broad category—for example, breaking down "Network Space and Governance Basics" into "Conceptual Foundation" and "Conceptual Framework." Finally, third-level coding isolates distinct concepts, statements, and illustrative examples that lend granular detail to each sub-theme, allowing for a comprehensive examination of specific governance practices, legal instruments, technological measures, and the evolving challenges within cyberspace security. This multi-tiered coding structure ultimately facilitates a more nuanced understanding of both the foundational principles of cyberspace governance and the complex, dynamic interplay of stakeholders, policies, and technologies that shape its ongoing development.

Moreover, this research method demonstrates a notable degree of scientificity and standardization, thereby enabling a comprehensive and incisive summarization of the book's innovative aspects, value propositions, and far-reaching significance. It systematically dissects the text to precisely pinpoint the novel contributions, assesses their academic and practical worth, and elucidates their implications within the relevant field, thereby providing a cogent and authoritative account of the book's overall importance and impact. Additionally, to more clearly delineate the book's central themes and key concepts, Python was employed to generate a word

cloud illustrating the most frequently occurring terms, as shown in **Figure 1**.

Figure 1. Word Cloud of the Book's High-Frequency Terms.

As shown in **Figure 1**, terms such as "governance," "threat," "international," "global," "challenge," "cooperation," "security," "cyberspace," "Internet," "comparison," and "framework" constitute a significant portion of the book's high-frequency vocabulary. These terms closely align with the subject keywords identified in this study. Text and word frequency analyses reveal the book's central focus on the complex dynamics of global cyberspace security governance. The prominence of these terms underscores the necessity of understanding multifaceted challenges and highlights the need for international cooperation and robust frameworks to address emerging cyber threats. Additionally, the recurring themes of comparison and governance suggest a critical evaluation of different countries' approaches and the development of cohesive strategies to enhance global cybersecurity.

4. The Innovation of This Book

The book achieves innovations in the research perspectives, methodologies, theoretical frameworks, practical applications, and contents pertaining to cyber security governance, thereby furnishing valuable insights and references for scholars, policy makers, and practitioners within the cyber security domain.

4.1. Research Perspectives Innovation

This book is not confined to the study of cyberspace security governance in a single country or region. Instead, it adopts a global perspective and comprehensively considers the situations of multiple countries and regions such as the United States, the European Union, Russia, Japan, Singapore, and India. By integrating the governance strategies of these regions with different political, economic, and cultural backgrounds into the same analytical framework, it presents readers with a comprehensive and diverse panorama of cyberspace security governance. This multi-dimensional and comprehensive perspective helps break geographical limitations, promotes international experience exchange and mutual learning, and provides broader ideas and references for global cyberspace security governance.

It integrates the knowledge and methods of multiple disciplines such as law, international relations, and information science. When analyzing cyberspace security governance issues, it not only uses legal theories to interpret international treaties and national laws but also explores the cooperative and competitive relationships among countries from the perspective of international relations. At the same time, it utilizes information science and technology to understand the characteristics and technical challenges of cyberspace. The interdisciplinary research perspective enables a more in-depth and comprehensive analysis of cyberspace security governance and can better address the multi-faceted problems in this complex field.

4.2. Research Method Innovation

It employs a systematic comparative research method to conduct a detailed comparison of the cybersecurity governance strategies of various countries. In the comparison process, it covers multiple key aspects such as legislative priorities, enforcement mechanisms, international cooperation methods, and technological investments. Through this comprehensive and in-depth comparison, it clearly identifies the strengths and weaknesses of different governance models, providing targeted and operable empirical evidence for countries to formulate and improve their cyberspace security governance strategies, which helps promote the development of global cybersecurity governance in a more scientific and effective direction.

In terms of data collection and analysis, it not only uses traditional qualitative analysis methods such as in-depth interpretation of text materials and case studies but may also attempt to introduce quantitative analysis methods (although the specific quantitative methods are not explicitly mentioned in the text, it can be speculated that there is such a research trend). By combining qualitative and quantitative methods,

it can more accurately grasp various phenomena and problems in cyberspace security governance, making the research conclusions more objective and reliable. Qualitative analysis helps to deeply understand the concepts, intentions, and sociocultural factors behind governance, while quantitative analysis can provide data support, reveal the scale, trends, and correlations of phenomena, and the two complement each other, jointly enhancing the scientific nature and persuasiveness of the research.

4.3. Theoretical Contribution Innovation

It conducts in-depth discussions and expansions on the theory of cyberspace sovereignty. In the current context of the globalization and virtualization of cyberspace, this book re-examines the concept, connotation, and extension of cyberspace sovereignty, analyzes the positions and practices of different countries on the issue of cyberspace sovereignty, as well as the causes and impacts of sovereignty disputes. Through these studies, it provides new ideas and viewpoints for the development of the theory of cyberspace sovereignty, which helps to better coordinate the interests and behaviors of countries in cyberspace at the international level and promote the establishment of a more just and reasonable cyberspace governance order.

Based on the comparative study of the governance strategies of various countries, this book may attempt to construct a universal framework for cybersecurity governance models. This framework integrates various elements such as law, policy, technology, and society, clarifies the roles and relationships of each element in cybersecurity governance, and provides a systematic theoretical guidance for countries to formulate and implement cybersecurity governance strategies. This model framework helps to improve the scientific and effective nature of cybersecurity governance and promotes the continuous improvement of the global cybersecurity governance system.

4.4. Practical Application Innovation

The research results can directly provide an important reference basis for governments of various countries in the process of formulating, revising, and improving cyberspace security policies. Through the analysis of the advantages and disadvantages of different governance models, policymakers can learn from successful experiences, avoid potential problems, and formulate cyberspace security policies that are more in line with their national conditions and the international situation, thereby improving the pertinence and effectiveness of policies.

The research in this book helps to promote innovation in international cooperation and coordination mechanisms in the field of cyberspace security. By in-depth analyzing the cooperation needs, interest demands, and challenges faced by countries in cyberspace security governance, it provides theoretical support and practical suggestions for the establishment of more effective international cooperation mechanisms. For example, in terms of information sharing, joint law enforcement, and technological research and development cooperation, the research results of this book can provide ideas and directions for cooperation among countries and promote the coordinated development of global cyberspace security governance.

4.5. Research Content Innovation

It pays attention to the impact of emerging technology developments in the field of cyberspace security and incorporates them into the research content. For example, when analyzing cybersecurity governance strategies, it considers the applications and challenges of emerging technologies such as artificial intelligence, blockchain, and the Internet of Things in areas such as network security protection, data management, and international cooperation. This timely follow-up of emerging technology trends makes the research content forward-looking and contemporary, and can provide advanced thinking and solutions for dealing with new problems in cyberspace security in the future.

When studying cyberspace security governance, it not only focuses on legal and technical issues but also conducts in-depth analysis of the influence of sociocultural factors on governance. Differences in the sociocultural backgrounds of different countries and regions will affect the public's awareness, attitudes, and behaviors regarding cybersecurity, which in turn will affect the implementation effectiveness of governance strategies. The in-depth research on this factor in this book fills the gap in previous research and provides a new perspective and content for a more comprehensive and in-depth understanding of cyberspace security governance.

5. Critical Perspective: Rethinking the Book

The book *Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implications* makes a notable academic contribution to the comparative study of cyberspace security governance. However, from a critical perspective, the book exhibits several areas that warrant deeper reflection and improvement.

5.1. Issues with the Representativeness of Country Selection

Although the book encompasses a diverse range of countries and regions, including the United States, United Kingdom, European Union, Russia, Japan, Singapore, India, and China, it lacks a thorough justification of the representativeness and rationale behind the selection of these countries. The backgrounds, resources, technological capabilities, and strategic objectives in network governance vary significantly among different nations. A simplistic horizontal comparison may overlook the underlying reasons for these differences, thereby limiting the generalizability of the conclusions. For instance, the analyses of emerging economies such as India and Singapore are relatively superficial, failing to delve into their unique challenges and innovative measures in network governance. This shortfall undermines the comprehensiveness and depth of the comparative study.

5.2. Limitations of the Theoretical Framework

The book predominantly relies on traditional legal and policy analysis frameworks, inadequately integrating the profound impacts of emerging technologies (such as artificial intelligence and blockchain) on cybersecurity governance. As technological advancements rapidly evolve, the threats and governance needs within cyberspace are continuously transforming. However, the book does not sufficiently analyze these technology-driven changes or their disruptive effects on existing governance frameworks, failing to elucidate the dynamic relationship between technological progress and legal norms. Furthermore, although the book attempts to incorporate an interdisciplinary perspective, this integration appears superficial in practice, lacking a comprehensive fusion of economic, social, and cultural dimensions. Consequently, the understanding of the complexities inherent in cybersecurity governance remains incomplete.

5.3. Insufficient Substance in International Cooperation Mechanisms

While the book emphasizes the importance of international cooperation in cyberspace security governance, it falls short in providing substantive recommendations and case analyses regarding specific cooperation mechanisms and implementation pathways. Cybersecurity issues are inherently transnational and complex, necessitating more detailed and actionable cooperative frameworks. However, the book's exploration of such content remains relatively vague, lacking concrete policy suggestions or successful case studies, which limits its applicability in practical policy formulation. Additionally, the book does not offer an in-depth critical analysis of power relations and interest conflicts within global network governance, inadequately revealing the profound impacts of great power rivalries and economic interests on cybersecurity cooperation.

5.4. Methodological Monotony

The book primarily employs qualitative analysis in its research methodology, lacking the support of quantitative data. This reliance on qualitative methods to a large extent affects the objectivity and persuasiveness of the research conclusions. Cybersecurity governance involves extensive data and complex dynamic processes, where quantitative analysis can provide more precise and verifiable conclusions. Future research could benefit from incorporating quantitative methods, such as statistical analysis and case studies, to strengthen the empirical foundation of the theoretical framework and enhance the overall scientific rigor and credibility of the study.

5.5. Neglect of Social and Cultural Factors

Cybersecurity governance is influenced not only by technological and legal factors but also by social and cultural elements. However, the book's exploration of these factors is relatively weak, insufficiently accounting for the varying understandings and expectations of cybersecurity across different cultural contexts. For example, there are significant differences in privacy protection laws and societal percep-

tions between Western countries and certain Asian nations, yet the book does not thoroughly analyze these disparities. This oversight affects the comprehensive understanding of the complexities in global network governance.

5.6. Lack of a Critical Theoretical Perspective

Although the book covers a broad range of topics, it lacks the in-depth application of critical theoretical perspectives[13]. Critical theory can uncover the underlying power structures and interest relations in network governance, revealing injustices and inequalities within existing governance frameworks. However, the book does not sufficiently explore these deeper issues, failing to use a critical lens to expose the potential contradictions and structural problems in cybersecurity governance.

6. Conclusion and Prospect

In sum, *Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implications* significantly contributes to the conceptual clarification, legal framework evaluation, policy model comparison, and strategic recommendations in the field of cybersecurity governance. By integrating textual analysis, comparative research, and qualitative data, the author illuminates the complexity of contemporary cyberspace governance through both legal and international relations lenses. Theoretically, the study synthesizes perspectives from international law, comparative law, and international relations[2, 4], while practically offering useful insights for states and international organizations to refine their governance strategies[1]. Additionally, the inclusion of a diverse range of countries, including the United States, United Kingdom, European Union, Russia, Japan, Singapore, India, and China, provides a broad overview of global network governance mechanisms, highlighting both commonalities and unique national approaches.

Despite its foundational contributions, future research could further investigate the governance challenges posed by rapidly evolving technologies—such as blockchain, quantum computing, and artificial intelligence—and their implications for international legal regimes[3, 6]. Building on the groundwork established by Li Zhi's analysis, scholars and practitioners can continue to enhance global governance frameworks and responsibly allocate roles and responsibilities, thereby ensuring a secure, stable, and sustainable cyberspace. Moreover, expanding the representativeness of country selection, deepening the theoretical framework to incorporate emerging technologies, and providing more detailed examinations of international cooperation mechanisms would enrich the study. Incorporating a greater diversity of methodological approaches and more extensively considering social and cultural factors would also enhance the comprehensiveness of the analysis. Additionally, integrating critical theoretical perspectives could offer a more nuanced understanding of underlying power dynamics and structural issues in cybersecurity governance. By addressing these aspects, the book's academic value and practical applicability can be substantially enhanced, fostering a more comprehensive and effective approach to securing the global cyberspace.

References

[1] Nye, J.S., 2010. Cyber power, 1–24. Harvard Kennedy School, Belfer Center for Science and International Affairs: Cambridge, UK.

[2] Finnemore, M., Hollis, D.B., 2016. Constructing norms for global cybersecurity. American Journal of International Law. 110(3), 425–479.

[3] Deibert, R.J., 2013. Black code: Inside the battle for cyberspace. Signal.

[4] Shackelford, S.J., 2014. Managing cyber attacks in international law, business, and relations: In search of cyber peace. Cambridge University Press: Cambridge, UK.

[5] Creemers, R., 2023. Cybersecurity law and regulation in China: Securing the smart state. China Law and Society Review. 6(2), 111–145.

[6] Kello, L., 2017. The virtual weapon and international order. Yale University Press: London, UK.

[7] Schmitt, M.N. (Ed.), 2017. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press: Cambridge, UK.

[8] Hathaway, O.A., Crootof, R., Levitz, P., et al., 2012. The law of cyber-attack. Calif. L. Rev. 100, 817.

[9] Roscini, M., 2014. Cyber operations and the use of force in international law. Oxford University Press: Oxford, UK.

[10] Samuel, G., 2014. An introduction to comparative law theory and method. Bloomsbury Publishing: London, UK.

[11] Hoecke, M.V., 2011. Methodologies of legal research. Which kind of method for what kind of discipline.

[12] Cane, P., Kritzer, H. (Eds.), 2012. The Oxford handbook of empirical legal research. OUP: Oxford, UK.

[13] Shuster, M., 2024. Critical theory: The basics. Routledge: London, UK.