ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 13, Issue 4, pp: (1-8), Month: October - December 2025, Available at: www.researchpublish.com

The Role of Cybersecurity in the U.S. Foreign Direct Investment National Security Review Mechanism and Policy Recommendations for Vietnam

Đỗ Quốc Bình [1]*, Prof. Nguyen Ba Dien [2]

[1*] PhD student, Faculty of Economic Law, Heilongjiang University in Harbin city, Heilongjiang province, China; Partner Development Assistant, NGS Telecommunication and Equipment Joint Stock Company; Lawyer, member of Hanoi Bar Association, Vietnam.

[2] Faculty of International Law, University of Law, Vietnam National University, Chairman of the Board of The Scientific Research Institute of Sea and Island (SRISAI), Hanoi, Vietnam.

DOI: https://doi.org/10.5281/zenodo.17257039

Published Date: 03-October-2025

Abstract: **This article systematically analyzes the development trajectory, evaluation criteria, and practical implementation of cybersecurity within the national security review process for foreign direct investment conducted by the Committee on Foreign Investment in the United States. The study demonstrates that cybersecurity has transitioned from a peripheral factor to a central pillar in Committee on Foreign Investment in the United States assessments, particularly in transactions involving critical technologies, sensitive data, and critical infrastructure. By continuously expanding review scope, refining risk assessment frameworks, and strengthening enforcement mechanisms, the United States has established the most comprehensive global system for evaluating cybersecurity in foreign direct investment. Building on this analysis, the article proposes policy recommendations for Vietnam to enhance its foreign direct investment cybersecurity review framework, including the development of a legal foundation, institutional mechanisms, risk evaluation protocols, and international collaboration.**

Keywords: **Cybersecurity; Foreign Direct Investment; National Security Review; Sensitive Data; Critical Infrastructure; Policy Framework.**

1. INTRODUCTION

The world is entering the Fourth Industrial Revolution, with the rapid development of cyberspace bringing immense benefits across many areas of social life, transforming the face of many nations and achieving remarkable breakthroughs for humanity. However, with the global nature and unlimited connectivity of cyberspace, which can be said to be unconstrained by space, time, and the social nature of cyberspace, it also poses significant challenges to the security of nations worldwide, such as cyber warfare, information warfare, cyberterrorism, and cybercrime. The development and mastery of cyberspace has become one of the most urgent tasks of great concern to many countries. Therefore, ensuring cybersecurity is a top priority, clearly reflected in the specific views, strategies, and actions of nations. US President Barack Obama once stated that cyber threats are becoming one of the most dangerous economic and national security challenges facing the United States. The internet has now become a weapon of mass destruction. Russian President Putin also affirmed that under current conditions, the destructive power of cyberattacks could be higher than that of any conventional weapon.

In the current era of digital technology and global economic integration, the role of cybersecurity is becoming increasingly important for foreign investment. Therefore, a national cybersecurity legal framework and evaluation standards in the field

of foreign investment are essential. The United States is the world's number one superpower, and cybersecurity and national security regarding foreign investment must be top priorities. That's also valuable experience for other countries.

2. MATERIALS AND METHODS

This study employs a qualitative and interdisciplinary approach, combining legal analysis, document research, and strategic policy evaluation. The results of the effectiveness assessment are based on understanding and analyzing the legal framework that United States has issued, such as the National Security Law, the Cybersecurity Law, the Data Security Law, the Cybersecurity Review Measures, and so on. Beside outlining the content and focus of cybersecurity assessments, as well as the implementation mechanisms and procedures, the author also presents several case studies to further strengthen the argument regarding the role of cybersecurity in United States national security assessment mechanism for foreign investment, thereby providing policy recommendations for Vietnam.

3. RESULTS AND DISCUSSIONS

1. Overview

1.1. Legal Basis and Role, Functions of Committee on Foreign Investment in the United States

The Committee on Foreign Investment in the United States is an interagency committee tasked with reviewing transactions involving foreign direct investment to assess their impact on U.S. national security [5]. Committee on Foreign Investment in the United States operates under laws and regulations such as Section 721 of the Defense Production Act (as amended) and the Foreign Investment Risk Review Modernization Act. Comprising cabinet-level members and officials appointed by the President, Committee on Foreign Investment in the United States is chaired by the Department of the Treasury and holds broad authority to evaluate transactions, impose conditions, and even recommend that the President block transactions deemed threatening to national security [3].

Committee on Foreign Investment in the United States's review scope has expanded from its initial focus on defense, telecommunications, and aerospace to encompass nearly all industries, particularly those involving critical technologies, critical infrastructure, sensitive data, and national security [20], [21]. The 2018 Foreign Investment Risk Review Modernization Act legislation significantly broadened Committee on Foreign Investment in the United States's jurisdiction, extending oversight to include non-controlling equity interests, certain real estate transactions, critical technologies and infrastructure, sensitive personal data, and critical supply chains [35].

1.2. The Role of Cybersecurity in Committee on Foreign Investment in the United States Reviews

Cybersecurity's role in Committee on Foreign Investment in the United States reviews has evolved from negligible to central. Initially, Committee on Foreign Investment in the United States assessments primarily focused on traditional defense security, but cybersecurity has now become a pivotal factor in evaluating foreign direct investment [26], [33]. The September 2022 Executive Order explicitly mandates Committee on Foreign Investment in the United States to assess cybersecurity risks during reviews, including potential cyber intrusions and malicious activities by foreign investors [12].

The 2023 Biden Administration Executive Order further emphasizes key issues requiring scrutiny, such as supply chain security, technological leadership, industry investment trends, cybersecurity risks, and personal data privacy [52].

This underscores that cybersecurity is no longer merely a technical concern but a core national security issue, intricately linked to economic security, technological competition, and geopolitical dynamics.

2. Legal Framework and Cybersecurity Evaluation Standards of Committee on Foreign Investment in the United States

2.1. Expanding the Definition of national security and Implications of Cybersecurity

Under the Committee on Foreign Investment in the United States framework, "national security" is a broad and evolving concept encompassing areas such as energy, defense, and technology [11]. In recent years, the United States has increasingly framed "economic security" as integral to national security, further expanding the scope of national security [22], [53]. This conceptual broadening allows cybersecurity assessments to be fully integrated into the foreign direct investment review process.

Committee on Foreign Investment in the United States evaluates multiple factors during its review, focusing on three core aspects: threat, vulnerability, and consequence [8]. (i) Threat: Relates to the intent and capability of the foreign investor, including the potential to conduct cyber intrusions or malicious cyber activities [18]; (ii) Vulnerability: Refers to the adequacy of cybersecurity protections and the susceptibility of U.S. operations to exploitation [16]; (iii) Consequence: Focuses on the potential impact of cybersecurity incidents on U.S. national security [17].

2.2. National Security Review Process and Cybersecurity Assessment

Committee on Foreign Investment in the United States follows a structured procedural process: Voluntary Filing: Parties involved in a transaction may voluntarily submit a notice to Committee on Foreign Investment in the United States. Preliminary Review (30 days): Committee on Foreign Investment in the United States conducts an initial assessment. Investigation (45 days): If risks are identified, an in-depth investigation is launched. Presidential Decision: The President finalizes the outcome [41]. Certain transactions (e.g., those involving critical technologies or sensitive data) may require mandatory filings [32], [34].

For cybersecurity, Committee on Foreign Investment in the United States conducts heightened scrutiny for deals involving sensitive data or critical infrastructure, often requiring detailed cybersecurity plans [1]. While no quantitative thresholds or specific metrics exist, robust cybersecurity measures can facilitate approval [1]. Committee on Foreign Investment in the United States integrates assessments from the intelligence community (IC) regarding the intent and capabilities of foreign investors, alongside evaluations of U.S. companies' vulnerabilities, to form an overall cybersecurity risk assessment [49].

3. Committee on Foreign Investment in the United States Cybersecurity Assessments

3.1. 2025 Trends and Developments

In 2025, Committee on Foreign Investment in the United States further intensified its review and enforcement efforts, including expanded jurisdiction, increased penalties, extended review timelines, and heightened scrutiny of specific countries [30]. Committee on Foreign Investment in the United States continues to prioritize emerging technologies (e.g., AI, quantum computing, semiconductors) and supply chain resilience [20].

On January 2, 2025, the U.S. Department of the Treasury implemented the National Security Strategy for Outbound Investment, prohibiting or restricting U.S. capital investments in sectors such as semiconductors, AI, quantum technologies, and other fields in specific countries [10], [13]. In February 2025, the White House issued a memo proposing Committee on Foreign Investment in the United States reforms and outbound investment review processes, easing scrutiny for allied nations while intensifying oversight of specific countries and expanding surveillance scope [14].

3.2. Cybersecurity Assessment Characteristics

Committee on Foreign Investment in the United States increasingly scrutinizes critical technologies and infrastructure, with a focus on cybersecurity risks [6]. Concerns center on risks that foreign acquisitions of critical hardware/software companies could create "backdoors" or malware [43]. Transactions involving sensitive data (particularly personal data) face stricter cybersecurity oversight, with Committee on Foreign Investment in the United States explicitly stating data security and access to sensitive personal information as priority areas [48].

Committee on Foreign Investment in the United States has ramped up enforcement and penalties for violations [6]. In 2025, the scope of industries requiring U.S. company filings with Committee on Foreign Investment in the United States expanded to include AI algorithms, quantum computing, biotechnology, 5G base stations, and cloud computing data centers [28]

4. Vietnam's Cybersecurity Landscape and U.S. Engagement

4.1. Vietnam's Cybersecurity Legal Framework

Vietnam enacted its Cybersecurity Law (2018) and related decrees (e.g., Decree No. 53/2022/ND-CP), imposing strict cybersecurity, data storage, localization, and foreign company operation requirements. The 2025 Cybersecurity Law (Draft) is currently under development and is expected to take effect in 2026. These policies mandate that sensitive data be stored domestically, significantly impacting foreign tech firms [4].

Vietnam's government evaluates foreign direct investment based on national security, antitrust considerations, and corporate approvals [37]. These policies align with Vietnam's WTO commitments, international or bilateral treaties, and domestic laws but lack a specific cybersecurity review mechanism [36].

4.2 U.S.-Vietnam Cybersecurity Collaboration

U.S. government and businesses have expressed concerns that Vietnam's Cybersecurity Law could hinder digital innovation, increase foreign direct investment costs, and disrupt data flows [2]. U.S. concerns about Vietnam's cybersecurity regulations are primarily raised within the WTO framework, rather than through bilateral agreements [50]. The U.S. Chamber of Commerce and other organizations have engaged Vietnam on cybersecurity issues, and the U.S. has shared information with Vietnam on undersea cable security [31].

The U.S. and Vietnam continue cybersecurity dialogue and cooperation, including memoranda of understanding (MoUs) and joint efforts to counter cyber threats [24]. For example, a collaboration framework was established between Vietnam's Ministry of Public Security and the U.S. National Security Council, as well as the Cybersecurity and Infrastructure Security Agency under the U.S. Department of Homeland Security [19].

5. Policy Recommendations for Vietnam

5.1. Strengthening Legal Frameworks and Review Mechanisms

Establish a Clear Cybersecurity Review System for foreign direct investment: Vietnam should draw inspiration from the U.S. Committee on Foreign Investment in the United States model and establish a specialized interagency committee to evaluate cybersecurity risks in foreign direct investment. This committee should define clear standards, procedures, and scopes for review. The scope should cover critical sectors such as critical infrastructure, sensitive data, and emerging technologies, incorporating both mandatory and voluntary filing requirements [51].

Balance national security and Investment Openness: Vietnam should avoid excessive restrictions that could deter foreign investment while safeguarding national security. Adopting a risk-based review approach similar to the U.S. model [8], would allow tiered assessments based on sectoral sensitivity and investor nationality, with streamlined processes for allied nations [27].

Refine Cybersecurity Evaluation Criteria: Develop detailed risk-assessment guidelines encompassing threat assessment (investor background, technical capabilities), vulnerability assessment (security measures of the target company), and consequence assessment (potential national security impacts) [29]. While full replication of the U.S. approach is unnecessary, Vietnam must establish a clear, context-specific framework.

5.2. Institutional Capacity Building

Create a Professional Technical Review Team: A specialized team comprising cybersecurity experts, data scientists, and industry specialists should provide technical support for foreign direct investment evaluations. Vietnam could emulate Committee on Foreign Investment in the United States practices by integrating intelligence agency assessments [15] to enhance collaboration between review bodies and domestic cybersecurity agencies.

Establish an Information-Sharing Mechanism: evelop a framework for cybersecurity information exchange between businesses, industry associations, and the government to improve review accuracy and efficiency. The U.S. CISA-private sector partnership model could serve as a reference [9] for sharing best practices and threat intelligence.

Enhance International Cooperation and Capacity-Building: Proactively seek collaborative support from nations like the U.S., Japan, and the EU to strengthen cybersecurity review expertise. While the U.S. has not issued specific recommendations for Vietnam, existing cybersecurity cooperation frameworks (e.g., with the national security Council) [46] provide a foundation for technical exchanges.

5.3. Data Governance and Cross-Border Data Flows

Implement Targeted Data Localization Requirements: Reassess the scope and necessity of data localization rules to avoid burdensome regulations that hinder the digital economy. Apply a tiered classification system, mandating local storage only for data directly tied to national security [25].

Establish a White-List Mechanism for Cross-Border Data Flows: Facilitate secure data transfers with trusted partners through a white-list system to boost trade and digital development. Vietnam could align with U.S. principles on digital trade rules [44] to balance security and growth.

Strengthen Personal Data Protection: Enhance legal frameworks and enforcement capabilities for personal data security to safeguard citizen rights and attract high-quality foreign direct investment. Vietnam should follow Committee on Foreign Investment in the United States's focus on sensitive personal data [7], [23].

5.4. Compliance Management and International Coordination

Promote International Rulemaking Coordination: Actively participate in discussions on digital trade and cybersecurity rules within multilateral frameworks like the WTO and APEC. Advocating for balanced global standards will reduce future adaptation costs for Vietnamese businesses [50].

Improve Policy Transparency and Predictability: Clarify cybersecurity and foreign direct investment review policies to provide foreign investors with clear expectations. Vietnam could emulate Committee on Foreign Investment in the United States's annual public reports [42] to build market confidence.

Introduce Compliance Incentives: Offer benefits (e.g., expedited reviews) to companies proactively adopting cybersecurity measures, fostering a positive compliance cycle. The U.S. practice of accepting detailed cybersecurity plans [1] as mitigation tools offers a valuable model.

4. CONCLUSION

The U.S. Committee on Foreign Investment in the United States framework, which integrates cybersecurity into national security reviews for foreign direct investment, exemplifies a high-level, comprehensive approach. By expanding national security definitions, refining evaluation standards, and strengthening enforcement, the U.S. has established a robust foreign direct investment cybersecurity review system. Key features include an expanding review scope, cybersecurity as a core evaluation pillar, sophisticated risk-assessment methodologies, and growing geopolitical influence.

For Vietnam, full replication of the U.S. model is neither feasible nor necessary. However, elements like risk-based assessments, institutional coordination, and compliance incentives offer valuable insights. While balancing national security with economic development and openness with risk prevention, Vietnam should gradually build a context-specific foreign direct investment cybersecurity review system, prioritizing legal frameworks, institutional capacity-building, and international collaboration.

As the digital economy and geopolitical dynamics evolve, cybersecurity reviews in foreign direct investment national security assessments will grow increasingly critical. Vietnam must proactively develop systems and capabilities to seize digital-era opportunities while safeguarding national security.

REFERENCES

[1] Ah Qiuqiuqiu, "*Cybersecurity and Corporate Governance: Data Leakage, Compliance, and International Investment*", CSDN, April 16, 2025, https://blog.csdn.net/weixin_42518874/article/details/147290408, Accessed on 23/9/2025.

[2] Alexander Botting, Elizabeth Guillot, *"Vietnam's Law on Cybersecurity: Bad on Cybersecurity, Bad for Vietnam"*, U.S. Chamber of Commerce, October 25, 2018, https://bitly.li/4v3k, Accessed on 23/9/2025.

[3] Anda Malescu, "*CFIUS Regulations: Comprehensive Overview for Foreign Investors in the US"*, Malescu Law, December 31, 2024, https://malesculaw.com/cfius-comprehensive-overview-for-foreign-investors-in-the-us/, Accessed on 23/9/2025.

[4] Angie.D, *""Overseas Daily, Tokopedia, the 'Indonesian Taobao,' secures $1.1 billion in funding from Alibaba and SoftBank; Line establishes joint venture with Thailand's largest digital bank, KBank", 36Kr, December 12, 2018*, https://36kr.com/p/1723053539329, Accessed on 23/9/2025.

[5] Bashar H. Malkawi, *"Chinese SOE Investment: An Economic Statecraft"*, Opinio Juris, February 7, 2019, https://opiniojuris.org/2019/02/07/chinese-soe-investment-an-economic-statecraft/ , Accessed on 23/9/2025.

[6] Benjamin G. Joseloff, George F. Schoen, G.J. Ligelis Jr., *" Foreign Direct Investment Regimes 2025"*, ICLG, Sixth Edition, Chapter 32, p.220-p.228.

[7] Camille Edwards, " A Primer on the Committee on Foreign Investment in the United States (CFIUS)", *Torres Trade Law*, July 1, 2025, https://bitly.li/1f4W, Accessed on 23/9/2025.

[8] Cathleen D. Cimino-Isaacs, Karen M. Sutter, *"The Committee on Foreign Investment in the United States"*, Congressional Research Service, Version 25, July 25, 2023. P.1-p.3.

[9] Charting R&D team, "*Cybersecurity VC Trends*", PitchBook, July 22, 2025, p.1-p.14.

[10] Chase Kaniecki, Samuel H. Chang, B.J. Altvater, and Ryan Brown, *"Long-Awaited U.S. Outbound Investment Regime Published, Will Become Effective January 2, 2025"*, Cleary Gottlieb, Alert Memorandum, November 4, 2024, p.1-p.11.

[11] Chen Qingming and Zhu Shaohui, "[Network Security Think Tank] Reflections on Industrial Control System Cybersecurity Review", Sohu, June 25, 2018, https://m.sohu.com/a/237712739_468736, Accessed on 23/9/2025.

[12] Chris Riotta, *"Biden adds cyber, data, supply chain risks to CFIUS reviews"*, Nextgov/FCW, September 15, 2022, https://bitly.li/U10l, Accessed on 23/9/2025.

[13] Client Alert, *"U.S. Outbound Investment Goes Live with Treasury Providing Additional Clarity—and European Outbound Investment Programs Get a Nudge Forward"*, Gibson Dunn, January 31, 2025, p.1-p.12.

[14] Client Alert, "*Trump Administration Signals Material Updates to CFIUS and Outbound Investment Regulations*", Gibson Dunn, February 26, 2025, p.1-p.6.

[15] Colin Costello, Andrew Gabel, Kate Applegate, *"ODNI Releases 2025 Threat Assessment: What it Means for CFIUS Reviews"*, Freshfields, 14 April, 2025, https://bitly.li/ZtQV, Accessed on 23/9/2025.

[16] Committee On Foreign Investment In The United States, *"CFIUS: Composition, Key Features, and Process"*, August 7, 2019, p.1-p.6.

[17] Congressional Research Service, *"The Committee on Foreign Investment in the United States (CFIUS)"*, June 27, 2018, p.1-p.66.

[18] Connecticut Bar Association , *"The Committee on Foreign Investment in the United States (CFIUS): Essentials for Lawyers (EDU230411)"*, April 11, 2023, p.1-p.73.

[19] DT, *"Minister To Lam receives high-profile professor from Harvard University"*, https://bitly.li/ZDbo, Public Security News, March 26, 2024, Accessed on 23/9/2025.

[20] G.J. Ligelis Jr. Christopher K. Fargo, Alyssa K. Caples and Margaret T. Segall, *"Chambers Global Practice Guides: Investing In... 2025"*, Chambers and Partners, February 11, 2025, p.813-p.834.

[21] Grace Hochstatter, *"Foreign direct investment reviews 2025: United States"*, White & Case, https://www.whitecase.com/insight-our-thinking/foreign-direct-investment-reviews-2025-united-states, Accessed on 23/9/2025.

[22] Gu Tianjie, "The Weaponization of Economic Interdependence and China's Response: From the Perspective of Coordinating the Promotion of Domestic and Foreign-Related Rule of Law", *International Law Studies*, No. 2, 2025, p.3-p.26.

[23] Hu Chen, *"Research on the Convergence of Foreign Investment Security Review Legal Systems in Europe and the United States"*, Beijing Law Review, Vol.16 No.2, June 2025 p.749-p.763.

[24] Huy Anh, *"Vietnam news in brief - March 26"*, Hanoitimes, Mar 26, 2024, https://bitly.li/JiBg, Accessed on 23/9/2025.

[25] ITI, *"ITI Comments on Foreign Trade Barriers for the 2025 National Trade Estimate (NTE) Rep"*, October 17, 2024, p.54-p57.

[26] Jeff Kosseff, *"Cybersecurity Law"*, Wiley, Second Edition, October 19, 2019, p.1-p.422.

[27] John Beahn, Bijan Ganji, Dara A. Panahy, Lafayette Greenfield, Lauren Trushin, Clay Melton, *"Trump Administration Proposes Significant Changes to CFIUS and the Outbound Investment Review Processes"*, Milbank, Global Risk & National Security Practice, February 24, 2025, p.1-p.4.

[28] Kimi@ingstart, *"2025 US CFIUS Review New Rules: Compliance Guidelines and Breakthrough Strategies for Chinese Investment in the US, TID Industry Risks and Structural Optimization"*, lngStart, https://www.ingstart.com/blog/30074.html, Accessed on 23/9/2025.

[29] Kristen Eichensehr , Cathy Hwang, *"National Security Creep in Corporate Transactions"*, University of Virginia School of Law, September 2022, p.1-p.64.

[30] Liu Yawei and Wang Xiaoya, "*Grandway Observation, Global M&A Market and Legal Changes (2022-2025H1)*", Grandway Law Firm, July 23, 2025, https://www.grandwaylaw.com/guofengshijiao/5248.html, Accessed on 23/9/2025.

[31] M. Faizal bin Abdul Rahman, *"Geopolitics meet Digital Security in ASEAN's Maritime Domain"*, Moderndiplomacy, April 16, 2025, https://bitly.li/0rY1, Accessed on 23/9/2025.

[32] Margaux J. Arntson, *"The United States' Foreign Direct Investment Screening Regime In A Post-Covid World"*, Review Of Banking & Financial Law, Vol.42 (2022-2023), p.429-p.473.

[33] O'Melveny, *"Biden Administration Issues Policy Directive on National Security Reviews of Foreign Investments in U.S. Businesses"*, September 23, 2022, https://bitly.li/SbY8, Accessed on 23/9/2025.

[34] Office of the Chief Counsel for International Commerce, Office of Investment Security, U.S. Department of Commerce, "*The Committee on Foreign Investment in the United States (CFIUS): Considerations for Foreign Direct Investment*", SelectUSA, Chapter 7, March 26, 2025, p.79-p.82.

[35] Oliver Borgers and Dominic Thérien, *"Panoramic Foreign Investment Review USA"*, Lexology, February 18, 2025.

[36] Oliver Borgers and Dominic Thérien, *"Panoramic Foreign Investment Review Vietnam"*, Lexology, February 1, 2024, p.1-p.16.

[37] Phuong Thi Minh Tran,Nam Ngoc Trinh, *"Foreign Investment Review 2021: Vietnam"*, Law Business Research, January 2021, p.159-p.164.

[38] Prokauer , *"2025 Proskauer Annual Review for Private Investment Funds"*, March 1, 2025, p.52-p.55.

[39] Qi'anxin Group, "*Dancing with Innovation, Walking with Value: Qi'anxin Releases Top Ten Cybersecurity Trends for 2025"*, February 8, 2025, https://mp.weixin.qq.com/s/8FKEemoyt8s9Gje3BvB0ng, Accessed on 23/9/2025.

[40] Riyadmedia, "*Vietnam Passes Sweeping New Cybersecurity Law"*, December 6, 2018, https://riyadmedia.com/news/2018/06/12/5570.html, Accessed on 23/9/2025.

[41] Shanghai Securities News, *"Characteristics of the Committee on Foreign Investment in the United States' Review*", Xinliang Finance, May 3, 2013, https://finance.sina.cn/sa/2013-05-03/detail-ikftpnnx6684709.d.html, Accessed on 23/9/2023.

[42] Simpson Thacher & Bartlett LLP, *"Report from Washington: Key Takeaways from the CFIUS Annual Report to Congress Covering Calendar Year 2024"*, August 11, 2025, p.1-p.4.

[43] Stephen Paul Mahinka, *"The CFIUS Review Process: Current Issues and Enforcement Trends"*, Moigan Lewis, November 11, 2015, p.3-p.56.

[44] U.S. Chamber of Commerce, *"The Next Stage of US-Vietnam Relations: A Blueprint to Deepen Trade and Investment Ties"*, May 08, 2019, https://bitly.li/HeY2, Accessed on 23/9/2025.

[45] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *"Department of Homeland Security Cybersecurity and Infrastructure Security Agency Budget Overview"*, April 1, 2024, p.1-p.24.

[46] Vietnam News, *"Cooperation between Việt Nam and US' IT companies could help combat cyber threats: Minister"*, March 26, 2024, https://bitly.li/Yc2E, Accessed on 23/9/2025.

[47] Wenwen Takes You to See the World, "*US Media: Vietnam Issues Cybersecurity Law Despite Sharp Criticism from US and EU*", NetEase, November 4, 2018, https://bitly.li/fH3N, Accessed on 23/9/2025.

[48] William D Torchiana, Marion Leydier and Nicholas F Menillo, *"Panoramic Insurance & Reinsurance 2025"*, Lexology, May 1, 2025, p.329.

[49] WilmerHale,*"M&A Report 2025"*, April 9, 2025, p.2-p.29.

[50] World Trade Organization, *"Minutes of the Meeting of 6–7 March 2019"*, Committee on Technical Barriers to Trade, 15 May 2019, p.36-p.38.

[51] Yang Fan, Yu Xiang, Liu Chuntong, and Yuanyuan, "*Zheng Chen's Policy: CFIUS: Concepts, Changes, and Impacts*", Sina Finance, September 18, 2022, http://finance.sina.com.cn/stock/stockzmt/2022-09-18/doc-imqqsmrn9562401.shtml, Accessed on 23/9/2025.

[52] Yicai Global, "*Biden orders tighter scrutiny of foreign investment, specifically targeting semiconductors, AI, quantum computing, and other sectors*", NetEase, September 16, 2022, https://bitly.li/Mt46, Accessed on 23/9/2025.

[53] Zhang Ming, "On the Generalization Trend of National Security in the Global Supply Chain and China's Response", *International Law Studies*, No. 2, 2025, p.130-p.148.