ISSN 2616-5783 Vol.7, Issue 11: 92-97, DOI: 10.25236/AJHSS.2024.071114

Research on the Legal Liability Distribution Mechanism of Cybersecurity under the Endogenous Security Concept of 6G Networks

Jiazheng Lv

Southwest University of Political Science and Law, Chongqing, 400000, China

Abstract: *This paper examines the restructuring of cybersecurity legal liability distribution mechanisms under the 6G endogenous security concept. It begins by analyzing the conceptual characteristics of 6G endogenous security and its challenges to traditional cybersecurity legal liability systems, highlighting the necessity for restructuring liability distribution mechanisms. Subsequently, it elaborates on the current cybersecurity legal liability distribution mechanism and its limitations in the 6G era. Building upon this foundation, the paper proposes four aspects of restructuring the cybersecurity legal liability distribution mechanism under the 6G endogenous security concept: diversified repositioning of liability subjects, dynamic division and coordination of liability scope, technologically intelligent liability determination standards, and innovative improvement of accountability mechanisms. Furthermore, the paper presents three legal countermeasures to ensure the effective implementation of 6G endogenous security liability distribution mechanism: improving legislation to establish a legal framework adapted to the 6G era, strengthening supervision to implement efficient technical support and monitoring mechanisms, and fostering innovation to facilitate a multi-party collaborative security ecosystem. These measures collectively aim to enhance the regulatory framework governing cybersecurity liability in the emerging 6G network environment.*

Keywords: *6G Networks, Endogenous Security, Legal Liability, Distribution Mechanism, Liability Restructuring*

1. Introduction

The emergence of 6G technology, with its endogenous security concept integrating security mechanisms into network architecture, presents unprecedented challenges to traditional cybersecurity legal frameworks. The integration of artificial intelligence and quantum computing in 6G systems introduces complex scenarios regarding liability distribution and responsibility attribution, particularly in an increasingly autonomous and global network environment.

This paper examines the relationship between 6G endogenous security and cybersecurity legal liability systems, analyzing current frameworks' limitations and proposing necessary reforms to accommodate 6G networks' unique characteristics while protecting stakeholder interests.

2. The Relationship between 6G Endogenous Security Concept and Cybersecurity Legal Liability

As a representative of next-generation communication technology, the endogenous security concept of 6G networks poses unprecedented challenges to traditional cybersecurity legal liability systems. Endogenous security represents not only technological innovation but also a fundamental transformation in security concepts, which inevitably affects the definition and distribution of cybersecurity legal liability. This section begins by examining the conceptual characteristics of 6G endogenous security, analyzes its challenges to traditional cybersecurity legal liability systems, and subsequently demonstrates the necessity of restructuring the cybersecurity legal liability distribution mechanism.

2.1. Conceptual Characteristics of 6G Endogenous Security

The 6G endogenous security integrates security mechanisms directly into network architecture as "Security as a Service."[1] Its core feature is endogeneity, where security becomes an inherent network attribute rather than an external function.[2] Two key components enable this: trusted engines for central security management and trusted enabling units for differentiated security configurations across communication entities.

Dynamic adaptability allows security mechanisms to evolve autonomously with technology advancement, independent of network generational evolution. The system employs intelligent autonomy through AI technology for automatic risk detection and handling. Using parallel companion networks and biological immune mechanisms, it conducts proactive security exercises to identify potential threats. The architecture achieves full-domain coordination through trusted engines and enabling units, providing comprehensive protection across traditional communication security and emerging services like AIaaS, DaaS, and wireless sensing.[3]

2.2. Challenges of Endogenous Security to Traditional Cybersecurity Legal Liability Systems

6G endogenous security presents fundamental challenges to traditional liability frameworks. The primary issue lies in defining liable entities within 6G networks, where security functions are distributed across various nodes, creating a diversified ecosystem. The collaborative operation of trusted engines and enabling units disrupts the traditional single-liability model, as operators, manufacturers, providers, and users collectively share security responsibilities.[4] This multiplication of liable entities demands new distribution mechanisms. Liability boundaries have become increasingly blurred due to the dynamic nature of 6G security, which enables flexible allocation of security functions among network entities. The differentiated capability configuration of trusted enabling units further complicates the clear definition of each party's liability scope, necessitating more adaptive boundary division methods.

Technical complexity presents another significant challenge, as intelligent security mechanisms require advanced technical knowledge from legal practitioners. Conventional methods struggle to evaluate the effectiveness of intelligent security measures or assess compliance in complex environments, requiring new technically-oriented liability standards. The traditional post-event accountability model fails to meet 6G networks' real-time protection requirements. As 6G security emphasizes prevention and immediate response, full-domain collaborative protection requires more proactive liability mechanisms. Additionally, 6G networks' global nature introduces complications due to varying laws and regulations across jurisdictions, requiring international consensus and cross-border collaboration mechanisms to effectively manage security liability in an interconnected network environment.

2.3. The Necessity of Restructuring Cybersecurity Legal Liability Distribution Mechanism

The profound challenges of 6G endogenous security necessitate urgent restructuring of the liability distribution mechanism to maintain network security and protect user rights. In the 6G network ecosystem, security liability bearers have expanded beyond traditional operators to include manufacturers, service providers, and end users. This new mechanism must establish a multi-party collaborative liability system that promotes fair responsibility sharing and active security participation.[5] Dynamic liability division is essential for responding to rapidly changing network environments, where AI-based assessment models and blockchain technology offer more objective and transparent processes for liability determination.[6]

The global nature of 6G networks necessitates international liability coordination mechanisms, establishing unified standards and cross-border enforcement mechanisms. This comprehensive restructuring, involving both legal adjustments and technological innovation, is essential for creating a robust legal liability system that supports 6G technology development. The adaptive nature of 6G endogenous security requires corresponding legal liability adjustments to ensure effective security governance in this evolving technological landscape.

3. Current Cybersecurity Legal Liability Distribution Mechanism and Its Limitations

As 6G technology advances, examining current cybersecurity legal liability distribution mechanisms becomes essential for understanding their adequacy in addressing emerging challenges and identifying necessary reforms.

3.1. Main Models of Current Cybersecurity Legal Liability Distribution

The current cybersecurity legal liability distribution follows a multi-subject sharing and hierarchical management model. Network operators bear primary responsibility under the Cybersecurity Law and Data Security Law, including security system establishment, technical measure implementation, and risk management.[7] Government departments execute supervision through cyberspace administration and public security organs, with the Measures for Cybersecurity Review establishing a top-down regulatory system.[8] This multi-level, multi-subject model creates a relatively complete liability system with clear boundaries among parties.[9] However, rapid technological advancement poses significant challenges to this traditional framework's effectiveness.

3.2. Challenges Faced by Traditional Liability Distribution Mechanisms in the 6G Era

Traditional cybersecurity liability distribution mechanisms face unprecedented challenges in the 6G context. The operator-centered model struggles to define liable entities as 6G networks introduce diverse participants like AIaaS and DaaS providers. The dynamic nature of 6G endogenous security further complicates liability boundaries, with security functions flexibly migrating between network nodes. Additionally, 6G networks' intelligent and autonomous characteristics demand more sophisticated liability determination standards, particularly for AI-human collaboration incidents.[10]

Cross-border coordination and preventive mechanisms present significant challenges, as existing frameworks struggle with multi-jurisdictional incidents and real-time protection needs. Traditional mechanisms inadequately address systemic risks like large-scale cyber attacks and cascading infrastructure failures, highlighting the substantial gap between current liability systems and 6G requirements.

3.3. Inadequacies of Existing Legal Framework in Adapting to 6G Endogenous Security

The existing legal framework shows significant limitations in adapting to 6G endogenous security. Current cybersecurity concepts fail to adequately capture 6G characteristics, with the legal definition of "network operators" unable to encompass new entities like intelligent service providers and edge computing providers.[11] While endogenous security demands dynamic liability distribution, current frameworks maintain static provisions that cannot address security function migration scenarios, often resulting in liability gaps or overlaps.[12]

New security challenges, including AI security and quantum communication security, lack specific regulatory provisions in current laws. Despite existing basic frameworks, they inadequately address 6G-specific risks and privacy protection in highly interconnected networks.[13] These limitations, coupled with insufficient cross-border enforcement mechanisms, necessitate comprehensive legal framework adjustments through collaborative efforts from legislators, technical experts, and legal practitioners.

4. Restructuring of Cybersecurity Legal Liability Distribution Mechanism under 6G Endogenous Security Concept

The evolution of 6G technology necessitates a fundamental reimagining of cybersecurity legal liability distribution mechanisms. This restructuring must address both current limitations and emerging challenges while establishing a framework capable of adapting to future technological developments.

4.1. Diversified Repositioning of Liable Entities

The 6G network environment demands a comprehensive repositioning of cybersecurity liable entities. The concept of "network operators" must expand to include emerging roles like AIaaS providers, DaaS providers, and edge computing service providers.[14] AI systems with autonomous decision-making capabilities require specific legal status, while users' evolving roles from consumers to data producers necessitate expanded responsibilities in personal data protection.

The emergence of specialized "security service providers" has become crucial to the 6G ecosystem.[15] Their professional status demands clear legal definition of responsibilities and obligations. This diversified repositioning creates an interconnected liability system where entities' responsibilities are mutually influential, better addressing 6G cybersecurity challenges while maintaining adaptability.

4.2. Dynamic Division and Coordination of Liability Scope

Under the 6G endogenous security concept, cybersecurity legal liability distribution must evolve toward a dynamic and collaborative system. Dynamic liability division, powered by real-time monitoring mechanisms and intelligent algorithms, automatically adjusts entities' liability scope based on network conditions. Collaborative liability fulfillment becomes essential as single entities cannot independently address all security challenges.

The "responsibility chain" concept effectively implements this dynamic approach, as security incidents in 6G networks typically involve multiple entities and stages.[16] Constructing responsibility chains links different entities' security obligations, while cross-domain considerations require international liability standards. The system must maintain flexibility to incorporate emerging security challenges through regular

4.3. Technologically Intelligent Liability Determination Standards

The 6G endogenous security concept demands technologically intelligent liability determination standards. This evolution requires precise quantification of network behaviors through measurable parameters like data transmission integrity, latency, and encryption strength. Advanced AI and big data technologies enable real-time analysis of network behaviors, complemented by "smart contracts" that automate liability determination procedures, enhancing efficiency and fairness.[17]

"Liability tracing" technology, through blockchain and distributed ledger systems, provides immutable records of network behaviors.[18] This ensures reliable evidence chains and prevents tampering in scenarios like cross-border data transmission. These technological innovations create a comprehensive framework bridging technical complexity and legal requirements in the 6G era.

4.4. Innovation and Improvement of Accountability Mechanisms

The 6G era demands a fundamental redesign of cybersecurity accountability mechanisms to address complex network environments and diverse security threats. The new system emphasizes both prevention and punishment, implementing a "security credit" evaluation system that monitors entities' security behaviors across technical measures, management systems, and emergency response capabilities.[19] Technology enhancement through AI and big data analysis enables rapid identification of responsible entities and security incident tracking, while blockchain technology ensures reliable evidence preservation and liability tracing. The accountability framework extends beyond traditional penalties to include targeted measures like mandatory technical training, security audits, and market access restrictions.

Global collaboration becomes crucial given the transnational nature of cybersecurity threats, requiring unified standards, cross-border investigation mechanisms, and international arbitration institutions. The system must maintain flexibility through regular assessments and adjustments to address emerging security challenges while balancing security requirements with innovation promotion. Through these comprehensive mechanisms and approaches, the accountability system can effectively address the complex security challenges of the 6G era while supporting technological development.

5. Legal Countermeasures to Ensure Effective Implementation of 6G Endogenous Security Liability Distribution Mechanism

5.1. Improving Legislation to Build a Legal System Adapted to the 6G Era

The effective implementation of 6G endogenous security liability distribution requires comprehensive legal system support. The primary task is updating legal concepts to encompass new participants and technological forms in the 6G environment, such as expanding "network operators" to include AIaaS and edge computing providers, and broadening "network security" to cover data and AI security. Systematic revision of existing laws like the Cybersecurity Law, Data Security Law, and Personal Information Protection Law is necessary to address 6G technology characteristics, requiring comprehensive optimization rather than mere additions.

Legislative coordination becomes crucial given 6G networks' complexity across multiple fields like communications, information technology, and data protection. A dedicated coordination mechanism is needed to ensure consistency and avoid conflicts between various laws.[20] The approach should combine principle-based and delegated legislation, establishing basic frameworks while allowing relevant departments to formulate specific technical rules. Additionally, the legislative process must incorporate multi-disciplinary expert consultation to ensure alignment between legal principles and technical realities, enhancing the law's operability and effectiveness in the 6G era..

5.2. Strengthening Supervision to Establish Efficient Technical Support and Monitoring Mechanisms

Under the 6G endogenous security framework, effective supervision is crucial for implementing liability distribution. Traditional methods cannot handle 6G networks' complexity, necessitating a technically-enhanced, intelligent supervisory system. Technology empowerment through AI and big data analysis significantly improves supervision precision, enabling regulatory bodies to monitor network status and identify risks in real-time.[21] This is complemented by distributed sensor networks and edge computing for rapid anomaly detection and response, while cross-domain collaboration facilitates international information sharing and joint enforcement against cross-border security threats.

The system requires dynamic adjustment mechanisms to keep pace with 6G technology evolution, including regular assessment and updates of supervisory methods and standards. Social co-governance expands coverage through industry self-discipline, public participation, and third-party security assessments. This comprehensive approach, combining technological advancement with collaborative supervision, not only enhances efficiency but also promotes proactive responsibility fulfillment among liable entities, ultimately creating a more secure 6G network environment.

5.3. Encouraging Innovation to Promote Multi-Party Collaborative Security Ecosystem

The effective implementation of 6G endogenous security liability distribution requires a security ecosystem encouraging innovation and multi-party collaboration. Innovation incentive mechanisms, supported by government funds for quantum communication and AI security research, alongside tax incentives for enterprises investing in network security, form the ecosystem's foundation.[22] Industry-academia-research collaboration and standardization efforts through international organizations like ITU and 3GPP enhance China's global influence.[23]

The introduction of Public-Private Partnership (PPP) models optimizes resource allocation through government and private sector cooperation.[24] This comprehensive ecosystem, encompassing innovation support, collaborative platforms, and standardization efforts, creates an environment where parties share both responsibilities and benefits in promoting 6G security development.

6. Conclusion

The transition to 6G networks necessitates a fundamental reconstruction of cybersecurity legal liability frameworks. Our research demonstrates that traditional mechanisms are insufficient for addressing 6G security challenges, and proposes reforms encompassing diversified entity positioning, dynamic liability division, and intelligent determination standards.

Implementation success requires coordinated efforts across legislation, supervision, and innovation, with particular emphasis on international cooperation. This transformation demands sustained collaboration among legislators, technical experts, and industry stakeholders to create adaptive liability frameworks that support secure 6G development while protecting all participants' interests.

References

[1] Liao Jianxin, Qi Qi, Wang Jingyu et al., 6G Intelligent Service Networking: Vision, Architecture, and Key Technologies. Sci Sin Inform, 2024, 54(5): 991-1024.

[2] Global 6G Technology Conference, White Paper on 6G Network Endogenous Security Architecture and Technology (March 9, 2023).

[3] Liu Guangyi, Zhang Huimin, Tong Zhou, et al. 6G Mobile Information Network Architecture: Transition from Communication to Everything as a Service [J]. Science China Information Sciences,

2024, 54(5): 1236-1266.

[4] Kazmi, S.H.A.; Hassan, R.; Qamar, F.; Nisar, K.; Ibrahim, A.A.A. Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions. Symmetry 2023, 15, 1147.

[5] Chen Bing. The Legal Dimensions and Development of China's High-Quality Digital Economy Development [J]. Journal of Shanghai University of Political Science and Law (Series on Rule of Law), 2024, 39(05): 72-94.

[6] Guo Chunzhen, Huang Yaopeng. Dual Asymmetric Cooperation: Operation and Optimization of Platform Content Governance Subject Responsibility [J]. Zhejiang Acad. J., 2024, 5: 78-92.

[7] Wang Siyuan. On Network Operators' Security Assurance Obligations [J]. Contemporary Law Review, 2017, 1: 101-115.

[8] Wu Weiming. Measures for Cybersecurity Review and the Construction of 'New Cybersecurity Concept' [J]. Information Security and Communication Privacy, 2020, 6: 25-35.

[9] Li Xinglin & Zhang Huimin. Constructing a Multi-subject Co-governance Model for Cybersecurity Prevention and Control [J]. Journal of Guangxi Police College, 2020, 2: 55-70.

[10] Guo Jing. Attribution of Responsibility Based on Human-Machine Joint Actors [J]. Studies in Dialectics of Nature, 2020, 36(11): 88-98.

[11] Weng Jie. On the Legal Definition of Network Service Providers in China [J]. Journal of Xinjiang Education Institute, 2017, 3: 122-135.

[12] Hong Yanqing, 'Management-Based Regulation' - Reconstruction of Network Operators' Security Protection Obligations Glob. L. Rev., vol. 4, 2016, 145-160.

[13] Wan Ke. Research on Legal Protection of Personal Information in the Context of Cybersecurity [D]. Southwestern University of Finance and Economics, 2020.

[14] Letaief, Khaled Ben et al., The Roadmap to 6G - AI Empowered Wireless Networks, ArXiv 1, 2019:1-20

[15] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang & Y.-D. Lin, Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges, IEEE Communications Surveys & Tutorials 201, 2021: 201-230

[16] Guo Chunxia. Product Safety Regulatory Game Based on Responsibility Chain [J]. China Securities & Futures, 2011, 6(6): 66-75.

[17] Chen Jidong. Legal Construction of Smart Contracts [J]. Oriental Law, 2019, 3: 112-125.

[18] Tang Yanjun & Xiao Changchun. Blockchain Assists Network Anti-corruption: A Technology-System Synergy Perspective [J]. Theory Herald, 2020, 10: 89-100.

[19] Zhang Baowen, Xu Xinhong, Kong Guodong, et al. Research on Credit Security Assessment System for Cyberspace Subjects [C]. Proceedings of the Third National Information Security Classification Protection Technology Conference, 2014: 156-170.

[20] Li Jia. On the Construction of Collaborative Protection Mechanism between Legal Norms and Technical Norms for Information Security [J]. Academic Exchange, 2014, 11: 78-90.

[21] Chen Tianying & Chen Jianfeng. Intelligent Big Data Security Supervision and System Implementation [J]. Communications of the ACM, 2017, 2: 45-55.

[22] Geng Tongtong. Establishing National Network Security Innovation Fund to Promote Leapfrog Development of Network Security Industry [J]. China Info. Security, 2016, (3): 34-45.

[23] Ji Xinsheng, Wu Jiangxing, Jin Liang, et al. Discussion on a new paradigm of endogenous security towards 6G networks [J]. Frontiers of Information Technology & Electronic Engineering, 2022, 23(10): 1421-1450.

[24] Hu Zhenhua, Liu Jingyue & Zhou Kongning. Research on Public-Private Cooperation Mechanism of PPP Model Based on Evolutionary Game [J]. Business Research, 2016, (7): 9-17.