Cyber Law as a Tool for Human Security: Legal Responses to Digital Threats

Xiaoyang Sun*

Faculty of Law, Australian National University, Australian Capital Territory, 2601, Australia

*luckyxiaoyang_sun@163.com

Abstract. In the digital era, cyberspace expansion brings convenience but also escalates threats like information leakage, infrastructure attacks, and transnational crime. This research explores cyber law's role in mitigating these risks. It categorizes digital threats into information security, cybersecurity, and cybercrime, analyzing impacts on individuals, society, and the state. Using GDPR and the Budapest Convention as case studies, it examines legal frameworks for data protection and crime combat. While effective, cyber law faces limitations: technological lag, jurisdictional conflicts, and balancing national security with individual rights. The research concludes that continuous global harmonization, proactive updates, and rights-respecting approaches are essential for resilience against emerging threats.

Keywords: Cyber Law, Human Security, Data Protection, Cybercrime, Digital Threats

1 Introduction

With the continuous development of Internet technology, big data and artificial intelligence have demonstrated outstanding potential and value. Cyberspace has evolved into a highly complex and dynamic emerging field, profoundly penetrating all dimensions of society. While bringing convenience to humanity, it also poses serious threats to human security. The security department of EMC, RSA, released quarterly security statistics and evaluations on online identity theft, phishing and malware, data leakage and data loss. The survey found that 23% of people worldwide would suffer from phishing attacks, and an average of one webpage would be infected every 4.5 seconds [1].

In the contemporary era of the digital economy, the rapid development of digital technology has also changed the legal landscape and given rise to the emerging field of cyber law [2]. People attempt to protect network security using various technical means but often find themselves unable to cope with the situation due to the limitations of protection technologies and the rapid update of network attack methods. Cyber law is the total of legal norms related to legal issues in cyberspace. It is a legal principle, regulation and legal theory system for managing activities in cyberspace. Also, it provides a framework for establishing legal norms, resolving disputes and enforcing rights and obligations in the network environment. As a regulatory means for cyberspace, how

T. Chamaratana et al. (eds.), *Proceedings of the 2026 12th International Conference on Digital Humanities and Frontiers in Social Sciences (DHFSS 2026)*, Advances in Social Science, Education and Humanities Research 1031,
https://doi.org/10.2991/978-2-38476-611-6_59

can cyber law, through legal mechanisms, deal with new threats in cyberspace to protect human security?

This research aims to explore how cyber law can provide legal protection for human security in the digital era and analyze its mechanisms and limitations in dealing with threats. This research conducts an analysis centered on the protective role of cyber law in human security in the digital era. It classifies the contents of contemporary cyber threats from one of the many classification perspectives and discusses the significance of cyber law in safeguarding information security, strengthening cybersecurity, and combating cybercrime at three levels; subsequently, through examples such as GDPR and the Budapest Convention.

2 Overview of Cyber Law and Human Security

2.1 The Current Situation of Cyber Threats

Threats to human security in cyberspace cover multiple aspects, such as personal, social, economic, and national security. They can be classified into three categories: information security threats, cybersecurity threats, and cybercrime.

Information security threats mainly target the security of unauthorized data and information, such as personal identity, financial information, and trade secrets, with a focus on the confidentiality and integrity of data. Common threats include privacy infringement and data leakage. During the data collection stage, due to the lack of standards, enterprises and platforms collect personal information without fully informing users, infringing upon users' right to know and choose. During the data storage stage, platforms may illegally disclose or sell user data [3]. For example, in the Cambridge Analytica incident in 2018, the personal data of 87 million Facebook users was collected and utilized without authorization for psychological profiling and targeted political advertising, making personal data an unregulated political tool.

The development of digital technologies and network platforms blurs the boundaries between personal information and public data, leading to increasingly unclear privacy boundaries. Personal information previously protected by law is now frequently leaked in extensive collection by the government, enterprises, and platforms. Technologies such as facial recognition and location sharing further exacerbate this trend. At the same time, privacy rights are regarded as tradable commodities in the Internet economy, and personal data is collected, analyzed, and sold, forming a vast data chain. AI and algorithm technologies also deepen the erosion of privacy, making individuals increasingly transparent in cyberspace.

Cybersecurity threats focus on network infrastructure security, aiming to prevent attacks from various parties that disrupt the system's operation. Critical infrastructure and new domain security issues directly relate to the lifeblood of the digital economy's lifeblood and cyberspace's stability. With the rapid development of network technology, critical infrastructure faces an increasing number of cyber-attacks and threats. Under this category, several forms, such as ransomware attacks and distributed denial-of-service attacks (DDoS), are relatively common. When critical infrastructure is attacked by hackers or DDoS attacks, DDoS attacks can cause disruptions to businesses and even

entire global locations, resulting in good-sized financial losses and harm to reputation. Cybercriminals can also use those assaults to extort cash from sufferers [4]. Such attacks can cause paralysis of websites, servers and even the entire network system, thereby affecting the regular operation of power, telecommunications, transportation and other systems and threatening social order and national security. Meanwhile, the development of emerging fields such as big data and cloud computing has brought about brand-new security challenges, expanding the network's attack surface.

Although there is no universally accepted definition of cybercrime worldwide, the standard view is that the core concern of cybercrime lies in the fact that the perpetrators use the Internet to carry out online illegal and criminal activities that affect the interests of individuals, enterprises and the state [5]. They aim at illegal profit or disrupting social order, usually including data crimes, network interference and destruction, and access crimes.

With the popularization of the Internet, cybercrime has been expanding. Victims not only include individuals but also enterprises and governments, and the economic losses caused have been continuously increasing. Cybercrime shows characteristics of organization and transnationality and often operates on a global scale in the form of groups. Cybercrime is more difficult to track than traditional crimes due to its fast technological updates, strong anonymity, and difficult evidence collection. Therefore, more advanced technical means and complete legal regulations are urgently needed.

2.2 The Significance of Cyber Law in Addressing Human Security Threats

The common perception among internet users is that some mobile shopping apps or social media platforms would push relevant products that they are interested in or recommend video content based on their browsing history. These are the results derived from analyzing the collected personal information through big data, aiming to enhance the accuracy of the information and meet various purposes of the platforms. However, the development of information technology has expanded the scope of leakage from individuals to enterprises and national secrets, which infringes upon personal rights and poses a threat to national security. Network threats come in various forms, such as information leakage, inference attacks, ransomware, phishing fraud, etc., with the frequency and complexity constantly increasing, highlighting the urgency of strengthening cybersecurity and risk prevention.

Ensuring Information Security: Protecting Data and Personal Privacy. Cyber law is of vital importance for the protection of data and personal privacy. It has established a basic mandatory legal framework for consent requirements, data privacy, etc. By applying the law, it restricts the collection, storage and analysis of personal information by institutions or platforms within a certain scope, mandatorily requiring them to adopt technical measures such as encryption and access control to prevent data leakage and abuse, and stipulating technical standards for data storage and transmission to ensure the confidentiality, integrity and availability of information. At the same time, cyber

law has promoted the clarification of the rights and obligations of multiple parties, such as data subjects (network platform users), controllers (enterprises) and processors (third parties), to a certain extent, determining the respect and protection of personal privacy rights in cyberspace.

Strengthening Cybersecurity: Protecting Network Systems and Infrastructure. With the acceleration of digitalization, hacker attacks have become increasingly rampant, and ransomware attacks have soared. Cyber law plays a crucial role in regulating network behavior and strengthening security protection. Traditional security mechanisms, such as firewalls and intrusion detection systems (IDS), have shown deficiencies in dealing with DDoS attacks, prompting the emergence of Software-Defined Networking (SDN) as a promising mitigation solution. However, with the increase in the number of connected devices and the continuous rise in network complexity, SDN controllers have faced significant challenges. With the widespread application of big data technology and the rapid development of information technology, new security vulnerabilities keep emerging, serving as entry points for hacker attacks. In reality, the limitations of technology and resources make security risks ubiquitous, ranging from operating systems, databases to network hardware. Sometimes, technology cannot adapt to the increasingly complex network environment and advanced threat forms in a timely manner. Against this backdrop, legal norms, as one of the comprehensive security strategies, can effectively enhance cybersecurity. Cyber law requires governments and enterprises to establish cybersecurity contingency plans to deal with sudden network attacks and conduct regular security assessments of important systems to prevent potential risks.

Furthermore, cyber law stipulates that enterprises must take protective measures to deal with network attacks that may paralyze servers, ensuring the normal operation of enterprises and reducing economic losses. Regarding DDoS attacks, cyber law requires service providers to deploy protection technologies and strengthen infrastructure security to counter the threat of large-scale malicious traffic attacks exploiting network vulnerabilities.

Cracking Down on Cybercrime: Maintaining Social Order and Public Security. The formulation of the Cyber Law has established a corresponding legal framework, clarified the legal responsibilities and punishment mechanisms, and intensified the severity of penalties, thereby providing a powerful legal deterrent for combating cybercrimes. Given that cyber threats have global characteristics, the coordination of cross-border legal definitions is particularly crucial [6]. A series of international conventions, represented by the Budapest Convention, aims to enhance legislation and promote international cooperation to strengthen the governance of cybercrimes. This convention emphasizes promoting collaboration among countries in law enforcement aspects such as cybercrime investigation, extradition of suspects, and intelligence sharing, to enhance cross-border crackdown capabilities and effectively curb the spread of global cybercrimes.

3 The Response Strategies to Cyber Law

3.1 Cyber Law and Data Protection

To address the increasingly severe information security and privacy issues in cyberspace, both national and international levels have formulated data protection and privacy regulatory frameworks. For instance, the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Chinese Personal Information Protection Law (PIPL), etc. The privacy protection laws in different countries and regions have their own focuses, but they all center on safeguarding individual data rights and are based on user consent as the legal basis. They explicitly prohibit default selection or covert collection and strictly regulate cross-border data flows.

The General Data Protection Regulation (GDPR) in the European Union is currently one of the most stringent data protection standards in the world. Just as mentioned earlier, the Facebook-Cambridge Analytica incident effectively responded to the deep-seated problems that were exposed by this incident and that pose a significant threat to human society. This significantly increased Facebook's data processing costs and legal risks, forcing it to make substantial changes in terms of user rights, transparency, etc.

In response to this risk, first, GDPR strengthens data sovereignty to counter privacy infringement and manipulation. It grants users rights such as the right to know, access, and the right to be forgotten in case of deletion of personal data, ensuring that individuals always remain at the core of the data processing process to strengthen users' control over data [7]. At the same time, GDPR stipulates that “users must explicitly consent (Opt-in)”, and enterprises cannot collect or share user data by default. This responds to the situation where users' data was applied without their explicit consent, violating the data protection principle.

Second, GDPR emphasizes limiting the secondary abuse of data to prevent the abuse of power and apportioning responsibility. It prevents secondary abuse of data through the “purpose limitation principle”, stipulating that data can only be used for the purposes declared at the time of collection and prohibiting unauthorized resale or use for political manipulation. At the same time, for Facebook's failure to promptly disclose data leakage situations and delay in fulfilling transparency obligations, GDPR clearly stipulates data transparency and notification obligations to prevent inducement-based authorization and misuse of purposes and requires that personal data processing should be appropriate and necessary to achieve the purpose of data processing.

Finally, GDPR imposes platform punishment and deterrence, constraining platform responsibilities. The regulation establishes a joint liability mechanism for data controllers and third-party processors to prevent platforms from “outsourcing” compliance risks. Moreover, it sets high fines to enforce compliance, stipulating that violations of GDPR can result in a maximum fine of 4% of global turnover, thereby strengthening enterprises' data protection obligations.

GDPR is a legal response to the human security in the digital society. It delineates the boundaries of data usage and the responsibilities of data controllers through legal

means and allows citizens the ability to resist the loss of personal privacy through institutions. It comprehensively checks information hegemony, data manipulation, and platform misconduct while ensuring personal privacy. This repairs the gap between technology and law and establishes a new standard for digital social governance globally. To further elaborate, the core value of GDPR lies not only in addressing the security threats brought about by the digital age itself but also in elevating data governance to the level of human dignity and social justice and integrating the protection of human rights in the digital context into a part of the modern human rights system. In an era where technology is increasingly advancing, and data has become a new type of asset, it is necessary to establish a strict data protection framework through laws, delineate power boundaries, and provide institutional tools against manipulation and algorithmic control for citizens' rights.

3.2 Cyber Law and Cybercrime

Apart from the issue of data privacy leakage, the increasingly serious nature of cybercrime also poses a considerable threat to human security. To address such threats, various countries have adopted specialized legal measures to regulate and combat them. The United States, through the Computer Fraud and Abuse Act, severely punishes cyber-attacks and cyber fraud. The European Union, through the Cyber-crime Convention, unifies the definitions and penalties for illegal access and system interference and other crimes among EU member states. China, through the Data Security Law (DSL), classifies data protection, severely punishes data activities that endanger national security and clarifies the criminal responsibility for illegal intrusion and data destruction in the Criminal Law Amendment. Australia's cybersecurity strategy emphasizes government, private sector and international cooperation. The 2001 Cybercrime Act and the recent Critical Infrastructure Security Reform are part of its legislative framework, aiming to protect the country from cyber threats.

Taking the Budapest Convention as an example, it is the cornerstone for international efforts to combat cybercrime. Its aim is to unify the legal definitions of various cybercrimes such as hacking attacks, online fraud, and cyber-terrorism among different countries and to promote cross-border law enforcement cooperation. From the perspective of criminal conviction, “cybercrime” is merely a general label used to refer to new types of crimes in the online information environment. The primary purpose of coordinating criminal convictions internationally is not to form a consistent definition of the crime but to encourage countries to classify online behaviors with social harmfulness as crimes and narrow the differences in criminal conviction and punishment among countries. However, the Philippine law at that time did not stipulate the development and dissemination of malicious software as a crime, so the parties involved could not be held accountable [8]. The Budapest Convention and its Protocols do not provide an interpretation of cybercrime but include crimes targeting information systems themselves, as well as fraud and forgery committed by means or conditions of network information technology.

Meanwhile, this convention has established a comprehensive international framework for combating cybercrime, emphasizing the necessity of harmonizing legal definitions and strengthening cross-jurisdictional cooperation. The convention highlights the importance of mutual assistance and promotes the establishment of a unified legal framework for combating cybercrime within the EU, enhancing the EU's ability to deal with cybersecurity threat. The police, with the help of the 24/7 cybercrime liaison mechanism established by the convention, promptly exchange information on suspects, server locations, and money flows and coordinate raid operations, successfully shutting down multiple illegal dark web websites and seizing a large amount of encrypted assets and data storage devices.

The legal basis provided by the convention breaks down sovereignty barriers, enabling seamless connection of multiple countries' criminal justice systems and achieving global suppression of cybercrime. At the same time, through unified definitions and evidence exchange mechanisms, it provides "soil" for member states to more effectively coordinate case tracking, significantly improving the detection rate of such crimes in international cooperation and safeguarding the basic human rights of vulnerable groups. With this international legal framework, cybercriminals can no longer hide beyond virtual boundaries.

4 Challenges and Limitations of Cybers Law Responses

Although Cyber Law has played an essential role in responding to the threats brought by the Internet space to human security, it still faces a series of problems and challenges during its implementation, which hinder the process of its effectiveness. Firstly, in the context of globalization, cybercrimes and data transmission often cross multiple countries and regions. However, there are differences in the law of cybersecurity and data protection among countries, leading to inconsistent practices in issues such as conviction, jurisdiction, and cross-border electronic evidence. The borderless nature of the Internet and the differences in legal norms make it difficult to solve cross-border cybercrimes relying on a single country and also bring compliance challenges for data management. Currently, international cooperation is still insufficient, lacking unified standards and enforcement mechanisms, and global collaborative governance urgently needs to be strengthened. Secondly, the current network legal system lags in responding to the rapid evolution of technology. Compared with the continuous evolution of new cyber threats and attack methods, legal norms often respond passively and are more reflected in post-event regulatory mechanisms. The current legal system fails to provide necessary legal support for these new security risks and vulnerabilities promptly, and many network problems cannot be solved on a legal basis, especially for emerging fields such as artificial intelligence, blockchain, and virtualization technology. Finally, how to strike a proper balance between "national security" and "individual rights" is also a major challenge. During the process of the country promoting the legislation on cybersecurity, it is inevitable that citizens' rights may be infringed upon and restricted due to the pursuit of national and social public interests. For instance, the law stipulates that network operators have the obligation to cooperate with government monitoring

and data storage requirements. The country may require Internet platforms to track users' online records in real time, review the content they post, and access these data without justifiable reasons. While safeguarding national security, this is likely to trigger strong opposition from human rights organizations and civil society regarding privacy infringement and the review system.

5 Conclusion

In conclusion, cyber law plays a crucial role in addressing human security threats. Through laws such as the General Data Protection Regulation (GDPR) and the Budapest Convention, cyber law has, to some extent, mitigated the risks brought about by aspects such as information security, cyber security, and cybercrime, providing a critical foundation for the security governance of cyberspace. However, its effectiveness is still constrained by the lack of global collaborative governance, the lag of legal norms, and the balance of rights. With the continuous development of digital technology, legal norms regulating cyberspace must also be continuously optimized. Only in this way can we better prevent the constantly changing forms of cyber threats and ensure the safety and stability of both the real and virtual worlds.

Reference

1. Saini, H., Rao, Y.S., Panda, T.C.: Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications 2(2), 202-204 (2012). https://www.researchgate.net/profile/Hemraj-Saini/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review/links/5422a5d00cf290c9e3a9ee9d/Cyber-Crimes-and-their-Impacts-A-Review.pdf
2. Babikian, J.: Navigating legal frontiers: Exploring emerging issues in cyber law. Revista Espanola de Documentacion Cientifica 17(2), 95 (2023). DOI:10.13140/RG.2.2.20264.55048.
3. Fire, M., Goldschmidt, R., Elovici, Y.: Online social networks: Threats and solutions. IEEE Communications Surveys & Tutorials 16(4), 2019-2024 (2014). DOI: 10.1109/COMST.2014.2321628.
4. Pillai, S.E., Vadakkethil, S., Polimetla, K.: Mitigating DDoS attacks using SDN-based network security measures. In: 2024 International Conference on Integrated Circuits and Communication System (ICICACS), p. 2. (2024). DOI: 10.1109/ICICACS60521.2024.10498932.
5. Ajayi, E.F.G.: Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems 6(1), 1-3 (2016). DOI: 10.5897/JIIS2015.0089.
6. Buçaj, E., Idrizaj, K.: The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews 8(1), 6 (2025). DOI: 10.31893/multirev.2025024.
7. European Parliament and Council: General Data Protection Regulation. Regulation (EU) 2016/679, 27 April 2016, OJ L 119, 1 (2016). http://data.europa.eu/eli/reg/2016/679/oj
8. Information Economy Report 2005, https://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf, last accessed 2020/02/09.gdpr-info.eu