**Aleksandra Nikolova Marković[[1]](#footnote-2)**

**NikoletaLutovac[[2]](#footnote-3)**

**Marko Milović[[3]](#footnote-4)**

**Legal Challenges in the Evolving Cyber security Landscape: National and International Perspectives**

**ABSTRACT**

The fast-changing character of digital technologies has resulted with many complex cybersecurity challenges that transcend national borders. This paper analyses the legal perspective of cybersecurity from both national, regional, and international levels, focusing on the evolving nature of cyber threats and the corresponding legal frameworks. This paper, also examines the existing legal frameworks and the challenges in implementing the cyber security law. Key challenges in cyber law enforcement include difficulty in obtaining electronic evidence, jurisdiction difficulties, slow legal adaption to new emerging threats, and the anonymity of the perpetrators. The paper concludes by proposing legal suggestions for improving the legal mechanisms for cyber defense through a multi-layered approach from international, state, and organizational levels. The need for enhanced international collaboration, the expansion of extradition networks, and the adoption of sector-specific cybersecurity legislation is highlighted in order for the states to show a higher level of resilience against cyber threats.

**Keywords:** *cybersecurity, cyber threats, challenges, legal perspective, international frameworks*

1. **Introduction**

The rapid development of information technology affects all spheres of individual’s lives, as well as all aspects of the operation of industries, and is the basis for their development. Information technology in the last two decades has experienced incredible growth and resulted withdigitalization of society, accelerated communication, globalization, and a change in the way of doing business. This exponential growth of information technology brings many challenges, ethical issues, and efforts for information security. With the evolution of information technology, cyber threats are becoming more innovative and sophisticated, which makes it difficult for legal systems to keep pace with the dynamic nature of cybercrime and ensure effective protection and law enforcement.As these threats become more complex and far-reaching, cybersecurity is no longer only a technical question. It has arisen as a significant legal issue, requiring robust legislative frameworks, international cooperation, and effective law enforcement mechanisms.

1. **Key Challenges in CybersecurityLaw Enforcement**

Due to the fast-changing character of cybercrimes and cyber threats, the legal system of every country is faced with critical challenges in practicing the law.

The first challenge is the difficulty in obtaining electronic evidence, specifically the lack of cooperation from service providers (Gupta and Lunia, 2024). This mainly occurs due to jurisdictional conflicts between countries. Service providers operate globally, but, laws differ from one country to another. In nations where the legal system is weak or where the cyber law does not exist or is not properly applied, providers may ignore requests. On the other side, large technology companies receive many requests to provide user data evidence, which can often lead to delays in processing and responding to such requests.

The next major challenge that cyber law enforcement faces is the delayed Legislative adaptation to the new emerging threats. The technology is changing rapidly every day, and cyber threats and attacks are increasing in complexity and specificity (Atrey, 2024). The judiciary system and professionals who are practicing the law constantly are one step behind the cyber criminals because they lack off appropriate tools to follow the new development of cyber-attacks. Furthermore, due to the fast-changing character of the technologies and cyber threats, it is practically impossible for lawmakers to constantly amend the law and keep pace with the newly emerging situation.

The anonymity of cybercriminals is also a serious challenge in practicing cyber laws and conducting proceedings against perpetrators of criminal offenses.Cybercriminals are hiding their identities by using advanced techniques and measures, in order to make it difficult for law enforcement to prosecute them (Bruner, 2019). Criminals are using stolen credentials and hide their real IP addresses by routing traffic through different countries.All of these challenges resultin delayed or failed investigations.

1. **Comparative Analysis of Legal Frameworks at the International, Regional, and National Levels**

This part of the paper will provide a comparative analysis of legal frameworks on international, regional, and national levels. Firstly, the most important international instruments will be analyzed, such as the Budapest Convention and United Nations initiatives. The primary objective of international initiatives is to establish internationally recognized rules and harmonize domestic legislation, while also emphasizing international cooperation. Afterward, the regional efforts, particularly within the European Union will be explained. Ultimately, the paper will examine how leading national governments have approached the legal regulation of cybercrime, data protection, and cyber defense.By analyzing similarities, differences, and challenges among these legal frameworks, this part of the paper will highlight the strengths and weaknesses of every approach.

1. **International Cyber security Frameworks**

The Budapest Convention on Cybercrime is the most significant and first international treaty, representing the collective response by the membersof the Council of Europe and a few non-member states to cyber threats (Nguyen &Golman, 2021).This Convention was adopted in 2001 in Budapest, Hungary, and was drafted by the Council of Europe, with participation from the United States, Canada, Japan, and other countries.The way jurisdiction is regulated in the Cybercrime Convention represents the most accurate and comprehensive expression of the current international legal framework on this issue (Vagias and Dougrat, 2014).The Budapest Cybercrime Convention, as an international treaty, is generally focused on harmonizing internet and computer-related crimes within national law systems, improving investigative techniques, and emphasizing international cooperation. Convention has been signed by numerous European and non-European countries, which makes this Convention one of the most significant and widely accepted international documents. However, some major states, like Russia and China have refused to sign, highlighting that the Convention was drafted without their participation and can impact the national sovereignty (Appazov, 2014). Therefore, countries that have not signed the Convention criticize its provisions as biased, arguing that they do not reflect their legal systems or national interests. One of the most problematic article of the Convention for the states that have not signed the Convention is Article 32. This provision allows a state party to access data across borders, even when the data originates from another country, without a strict obligation to inform the authorities of that country. This could lead to violations of state sovereignty in the digital realm (Danelyan and Gulyaeva, 2020).

The United Nations has made efforts to combat cyberattacks, from passing resolutions to establishing ad hoc bodies. All UN efforts to combat cyberattacks are aimed at helping states build their own resources for defense against cyber threats.The UN General Assembly has adoptedmany resolutions on the use of ICTs concerningcyber security. The main points that are addressed in the resolutions are (Arif, 2020):

* Promote the usage of cyberspace solely for non-aggressive purposes.;
* Encourage states to retrain from organizing or engaging in hostile cyber activities;
* Cooperation for capacity building, especially in developing countries.

Although the UN has brought many resolutions regarding cyber security and their bodies are proactive in improving the national capacities for defense from cyber-attacks, still, several challenges remain. The main challenges are the lack of mechanisms for enforcing the norms provided in the Resolutions and the differences in the approaches between countries that are advocating state sovereignty (e.g., Russia, China) and those advocating free and open cyberspace (U.S., EU).

1. **Regional Frameworks**

**Regional cybersecurity frameworks** are the results of the efforts of the states positioned in a certain geographic areathat share similar challenges in cyber law enforcementand aim to harmonize their legislation. These frameworks include joint **policy coordination, information sharing,** and**capacity building.**

**European Union.**Regarding the European Union's efforts to determine a framework related to cyber security, the two most important documents will be analyzed: **The Directive on Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR).**The NIS Directive was adopted by the European Union in 2016 and later updated with NIS2 in 2022. This Directive is the first wider EU document with the main aimof supporting cybersecurity through the state’s critical infrastructure. Member States must ensure a high level of network and information security, by establishing national strategies, competent authorities, and incident reporting obligations for operators and digital service providers (Markopoulou et al., 2019). Despite its importance, the directive faces several challenges. One of the biggest challenges is the disproportional level of implementation between Member States, which can lead to uneven standards of cyber protection. Consequently, these discrepancies may lead to legal uncertainties for organizations operating across borders, by underminingincident response efforts and undermine the strength of the EU’s collective approach to cybersecurity in general.

General Data Protection Regulation is maybe the most important document which addresses the protection of individual personal data. It providesvery strict rules on how to collect personal data, and how to be processed, stored, and shared by imposing notable obligations on organizations. GDPR applies to every organization inside the EU or outside the EU that handles the personal data of EU citizens. This regulation provides severe fines for non-compliance. Fines are reaching up to €20 million or 4% of global organizational annual turnover, whichever amount is greater.This Regulation led to high compliance costs for businesses (Smirnova and Morales, 2024), but its implementation is from a significant meaning in today’s digital landscape.

1. **National Cybersecurity Frameworks**

**China.**China has developed a comprehensive cybersecurity and data protection regime grounded in three key laws: the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL). These laws establish strict controls over data processing, cross-border transfers, and the protection of critical infrastructure, often with extraterritorial reach. The CSL is the most important law regarding the establishment of cyberspace sovereignty. Additionally, Cybersecurity Lawrequires data localization on the territory of China for “critical information infrastructure operators,” that are operating on the territory of China, regardless if they are local or foreign companies (Jiang, 2021).The DSL is focused on the protection of data during processing, and PIPL provides a framework for how personal information should be handled and safeguarded (PwC, 2022).To conclude, the cyber laws of Chinaemphasize data sovereignty with strict government approval for sharing data with foreign authorities and providehigh penalties for non-compliance.

**United States of America.** In the United States, cyber security laws and regulations are sector-specific, fragmented, and driven by both federal and state levels. The U.S. does not have a single, comprehensive national cybersecurity law, but, several key federal and state laws and guidelines play crucial roles (Joshi, 2024). Key federal laws include the Computer Fraud and Abuse Act (CFAA), which criminalizes hacking, the Cybersecurity Information Sharing ACT (CISA), which emphasizes public-private threat intelligence sharing, the NIST Cyber security Framework (CSF) by the U.S. National Institute of Standards and Technology, which is used globally as a best-practice guide due its clear and flexible structure and serves for risk-based cyber security planning. There are also many important sector-specific laws with the main goal of defending and protecting the critical sectors.

1. **Legal Mechanisms for Cyber Defense: From Prevention to Prosecution**

Cyber defense requires a multi-layered legal approach that spans international cooperation, national legislation, and organizational policies. In this part of the paper recommendations for improving the states' mechanisms for cyber defense will be provided.

On the international level, strengthening international cooperation between countries to exchange information and establish global databases on cyber threats could be an important step for joint efforts of the states against increased cyber threats. Also, another proposal for the state could be establishing an international joint cybercrime enforcement team that can intervene more effectively in preventing cyber-attacks or, if an attack occurs, to prosecute the perpetrators more quickly and effectively. Furthermore, expanding the network of extradition treaties between countries is a crucial recommendation to strengthen the international cooperation between states against cyber threats. By expanding the network of thesetreaties, states can more effectively pose a request for the transfer of cybercriminals. Moreover, a wider extradition network will support mutual legal assistance in conducting investigations.

On the national level, governments need to put the defense from cyber-attacks as a national priority. By putting this question as a strategic national interest, the government is protecting its citizens and their personal information. One of the suggested measures that governments should consider is establishing a National Cyber Security Agency. This Agency will serve as a central authorityfor cyber defense and for analyzing cyber threats. Another proposal is the adoption of special cyber security laws for protecting critical sectors (such as energy, banks, healthcare, etc.).By adopting these laws, governments can provide implementation of measures that will be minimum cybersecurity standards for organizations. Also, organizations will have an obligation to report data breaches or cyber incidents promptly and adopt incident response plans.Governments will successfullydefine responsibilities, defensemechanisms, and penalties for non-compliance, which will protect the important sectors from different attacks. The next proposal is for Governments to invest in training Law enforcement for cybercrimes by providing them with modern tools to respond to cyber threats and to develop resilient cyber defense systems. Last, but not least proposal is that the Government should organize Cyber Awareness programs for its citizens to educate them to spot phishing emails, to use password managers, etc.

On an organizational level, organizations can undertake some measures to protect themselves from cyber threats and attacks. Every organization should establish detailed internal procedures for fast reporting any data breach. Next, it should train employees how to recognize phishing emails or other cyber threats and follow industry-specific laws for cyber protection. By adhering to these measures, major damages resulting from cybercrime can be prevented.

1. **Conclusions**

This paper has examined the evolving landscape of cybersecurity law, highlighting the complex challenges related to obtaining evidence, jurisdiction, and the anonymity of cyber criminals.Also, a critical review of the legal regulation at the international, regional, and national levels was made. Although many efforts have been made at the international, regional, and national levels to protect states and their citizens from cyber threats and attacks, the rapid development of technology, and with it the complexity of cyber-attacks, make the process more complicated. The fast-changing nature of information technology brings many positive opportunities for development, but at the same time makes it almost impossible for legal regulation to follow that development, adapt to new technologies, and provide protection. Ultimately, strengthening cybersecurity is not solely a technical or legal task, moreover, it is a shared global responsibility that demands coordinated action, mutual trust, and continuous legal cooperation. Only through multi-layered collaboration at all levels (governmental, regional, and international) the legal system can become a truly effective tool in defending against cyber threats and securing the digital future.

1. **References**
2. Arifi, D., Arifi B. (2020). Cybercrime: A Challenge to Law Enforcement. *SEEU Review*, 15(2), 42-55.
3. ArturAppazov. Legal aspects of cyber security, University of Copenhagen, 2014, 1-70.

# Atrey, I. (2024).Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*, 10(3), 1-15.

# Bruner, M. (2019). Challenges and Opportunities in State and Local Cybercrime Enforcement. Journal of National Security Law and Policy, 10(1), 563-582.

1. Danelyan, A., Gulyaeva, E. (2020). International Legal aspects of cybersecurity. *Moscow Journal of International Law,* 1(1), 45-53.

# Gupta, J. and Lunia, U. (2024). Cyber Crime and the Challenges of Prosecution and Prevention. *International Journal of Law Management and Humanities,* 7(4), 1038-1052.

1. Jiang, M. (2021). Cybersecurity Policies in China*.CyberBRICS: Cybersecurity regulations in BRICS countries*, 195–212.
2. Joshi, A. (2024). Study of Cybersecurity Laws and Regulations. Indian Journal of Law, 2(3), 7-14.
3. Markopoulou, D., Papakonstantinou, V.and de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 1-11.
4. Nguyen, C., Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries ‘Law on the books’ vs ‘law in action’. *Computer Law & Security Review*, 40 (1), p. 1-13.
5. Smirnova, Y., &Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: A systematic literature review. *International Journal of Law and Management*, 66(3), 326–344.
6. Vagias, M., Dougart, S. (2014). The territorial jurisdiction of the International Criminal Court. Cambridge, UK: Cambridge University Press, Cambridge University, p.160
7. Wand, V., Xinyao, Z., Wang, E. (2022). A comparison of cybersecurity regulations: China. [Online]. PwC. Last updated: 19 October 2025. Available at: <https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html> [Accessed 24 May 2025].
1. Associate Professor, Faculty of Law, Megatrend University, anikolova@megatrend.edu.rs [↑](#footnote-ref-2)
2. Associate Professor, Faculty of Law, Megatrend University, nlutovac@megatrend.edu.rs [↑](#footnote-ref-3)
3. Associate Professor, Faculty of Law, Megatrend University, mmilovic@megatrend.edu.rs [↑](#footnote-ref-4)