Marković M. Darko[*]
https://orcid.org/0000-0001-9124-6417
Marković Darija[**]
https://orcid.org/0000-0001-5602-902X

UDK: 343.326:004
Original scientific paper
DOI: 10.5937/ptp2502049M
Received on: April 8, 2025
Approved for publication on:
April 29, 2025
Pages: 49–61

CYBERCRIME AND LAW – MANAGING CHALLENGES AND PROSPECTS IN THE DIGITAL AGE

ABSTRACT: Cybercrime has emerged as a global threat in the digital age, posing significant challenges to legal systems worldwide, particularly in terms of their effectiveness and applicability. This paper examines how these challenges are addressed within international and national legal frameworks, highlighting key obstacles and offering perspectives for improvement. It reviews existing legal mechanisms, such as the Budapest Convention, the General Data Protection Regulation (GDPR), and national legislation in Serbia, and evaluates their adaptability to contemporary technological threats and potential for reform. The research adopts an interdisciplinary methodology, combining theoretical analysis of international and domestic legal texts with empirical examination of statistical data and case records. Practical challenges of legal enforcement are assessed through a systematic review of relevant sources, including the number of reported cyberattacks, and insights drawn from Interpol and Europol reports.

The findings highlight systemic challenges, such as jurisdictional limitations, ineffective laws, and insufficient technical capacities. Proposed solutions emphasize enhanced international cooperation, modernization

[*] PhD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: darko.markovic@pravni-fakultet.edu.rs

[**] Msc, PhD candidate, RUDN University, Law Institute, Moscow, Russia, e-mail: darija.dm.markovic@gmail.com

of legal frameworks, investment in technology, and public education. The paper concludes that building legal resilience to cybercrime requires a coordinated international effort to address legal and technological vulnerabilities exploited by cybercriminals.

Keywords: *cybercrime, law, digital age, jurisdiction, international cooperation.*

1. Introduction

When thinking about cybercrime, it is simply unthinkable not to see how much of a daily risk it has become – it is no longer a question of if it will happen, but when. Cybercriminals aren't just someone breaking into your computer and taking your password; it's a whole world of fraud, theft, and even endangering the security of countries. In order to even discuss what cybercrime is, one must first clarify what is included in that term. In a general interpretation, cybercrime includes malicious activities such as identity theft, unauthorized access to personal data and their misuse for the purpose of false representation, for example with the aim of stealing money or taking a loan on the account of the victim. Phishing is a widely known concept – e-mail users often receive e-mails that "inform" them that they must submit their account information, while banks warn them not to fall for such scams. Ransomware is an insidious threat – the hacker locks files and demands a ransom, and if the victim doesn't pay, they lose everything. DDoS attacks flood the server with requests until the site goes down, and social media scams involve fake messages that trick the user into clicking on a malicious link.

According to a report by Cybersecurity Ventures, the global cost of cybercrime is expected to reach $10.5 trillion annually in 2025, three and a half times more than in 2015 (Esentire, 2024) – that's more than the GDP of many countries! Ransomware attacks are sometimes taken lightly, on the principle of "it's not me, who cares about me". Nevertheless, it is a danger that is spreading, growing from year to year, and practically no one can be sure that he will not be the subject of such an attack and blackmail tomorrow. In the last five years, this risk has increased by numbers that are equally ruthless – the number of these attacks has increased by as much as 150% in the period from 2020 to 2025 (Griffiths, 2025). What does this mean in practice? That every day at least one company or at least one individual is a victim of such an attack. Or, more precisely, it happens every 14 seconds (Palatty, 2025). One in a sea of examples of such criminal acts occurred in

2021 in the USA, when hackers broke into the Colonial Pipeline system and locked it, then demanded a ransom, and while waiting for a solution to this problem, there was a fuel shortage on the East Coast (Easterly & Fanning, 2023). Or the Facebook data breach in 2023, when millions of users' data was leaked to the dark web (Behera, 2023). One might ask: "What's the use of my data, I'm not a famous person on the Internet". The answer could be quite unpleasant, just like in the aforementioned attack in 2023, when "unknown" people were also sent fake messages for months, causing them to lose money. These cases highlight the turbulence that cybercrime can cause in an individual's personal life or the functioning of a state. The financial losses are enormous – companies lose billions, and individuals often lose everything they have. However, those who have found themselves in similar predicaments know that it is not just about money. Because how can you pay for that feeling that someone, and not just anyone but a criminal, stole your identity and took away your privacy? The threat to national security is far more extensive, because the consequences are also more severe, often on a huge scale, as happened in the case of the attack on Estonian servers in 2007 (see Samsoerizal, Hidayat & Sukendro 2022). We have a drastic example of such attacks in the locking of hospital computer systems by hackers during the 2020 pandemic (He, Aliyu, Evans, & Luo 2021). Who can say in such moments that it is only about money when human lives are at stake? With all of this in mind, it's not hard to see that cybercrime isn't just a technical problem – it's a social problem, changing the way we trust each other, how we function as a community, and even how countries protect their citizens. With all these figures and cases, the question remains – how to deal with this, when everything happens at the speed of light, and criminals are always at least one step ahead?

Legal systems struggle with great restrictions when trying to react to this threat. Among the difficulties include the multinational character of cybercrime, obsolete legislation, technological backwardism, and the clash between privacy and security. The purpose of this paper is to investigate how current legal systems handle these issues, spot main challenges and provide fixes. Combining statistical data and case studies with the analysis of national and international legal actions, the study uses an interdisciplinary approach. Along with reports from agencies like Interpol and Europol, the methodological process consists in an examination of pertinent materials including the Budapest Convention, GDPR and national legislation of Serbia. By considering the legal frameworks and obstacles in their application, the aim of the paper is to help find solutions by which the law could more successfully control cybercrime..

2. Legal frameworks for cybercrime

If any crime is a global threat, then the same can be said for cybercrime, which increases the importance of establishing appropriate legal mechanisms. This need exists because the existing legal mechanisms are not sufficiently developed due to the major limitations of legal systems, primarily in terms of enforcement and efficiency. Perpetrators, their victims and infrastructure are often under different jurisdictions, and the international nature of these crimes poses a key burden in the search for applicable solutions. By studying current national and international legal systems, we can see the complexity of these issues, but also see directions in which we could go further.

Adopted in 2001 by the Council of Europe, the Convention on Cybercrime, sometimes known as the Budapest Convention (Council of Europe, 2001), is one of the main international papers for the fight against cybercrime. This agreement compels participating governments to enact legislation that prohibit illegal access to computer systems, data theft, computer fraud and similar crimes, therefore being the first attempt to create a shared legal framework to combat cybercrime. The Convention underlines especially the value of international collaboration in investigations, including information exchange and extradition. More than 70 states, including Serbia, which joined in 2009, had signed this convention by the beginning of this year. However, major challenges remain. Unfortunately, the global system is seriously compromised by the fact that large countries like China and Russia are not signatories, and past practice tells us that massive cyberattacks have often been linked to their infrastructures or citizens. Furthermore, the Budapest Convention was approved more than twenty years ago at a period when major ransomware assaults, the dark web, and cryptocurrencies were inconceivable. This begs the issue of whether this paper can handle contemporary problems include tracing anonymous bitcoin transactions or defending against attacks on important infrastructure.

Extra legal tools have been created inside the European Union to strengthen the battle against cybercrime. Adopted in 2016 and entered into force in 2018, the General Data Protection Regulation (GDPR) set rigorous criteria for the protection of user privacy (European Parliament and Council, 2016), therefore requiring businesses to guarantee the security of personal data. Regarding data leaks, the fines are substantial; for instance, a technology corporation in Ireland paid 1.2 billion euros for poor customer data protection in 2023 (Beveridge, 2023). But GDPR's main focus is safeguarding privacy, not actively fighting cybercrime, which restricts its applicability in this sense.

On the contrary, the NIS2 Directive, adopted in 2022 and approved in 2023, seeks to enhance the cyber security of EU vital infrastructure like hospitals, electricity grids and water systems. This directive mandates member states create national plans guaranteeing a quick reaction to events and safeguarding against cyberattacks. The NIS2 Directive's implementation is challenging, nevertheless; many nations – including certain EU members – have limited resources, specialists, and technical capacity to carry out these policies, therefore impeding development.

Legal actions pertaining to cybercrime exist in Serbia at the national level, however their efficacy is dubious. The 2016 Law on Information Security mandates public organizations and businesses to create mechanisms to stop cyberattacks and lays down guidelines for data protection. Article 301 of Serbia's Criminal Code forbids illegal access to a computer system, with a penalty of up to five years in prison, therefore addressing computer fraud. Still, the application of these rules runs several challenges. The absence of skilled staff is one of the main issues; in Serbia, there are few forensic professionals qualified to carry out thorough investigations about cybercrime. Furthermore, courts sometimes lack understanding of the technological features of these cases; how would you explain to a judge what blockchain is or how bitcoin transaction monitoring operates? This gets even more difficult when the perpetrators are from aboard since the Serbian court system lacks systems for efficient collaboration with other nations in such circumstances.

Variations in rules across countries present another major challenge. Imagine a situation where a Russian hacking group targets a German corporation using servers in the Netherlands, and the ransom money ends up in cryptocurrencies on a Singapore stock exchange. Which country has the jurisdiction to act and pass judgment? Germany, because its corporation is the victim? Russia, because the hackers are operating from where? The Netherlands, because its servers were used? Or Singapore, because the money landed there? Until countries agree on this, the perpetrators usually disappear without a trace. Europol said in 2024 that a large number of cyberattacks still go unsolved, mainly because of these problems: hackers mask their actions using VPNs, the dark web, anonymous payment methods (Eurojust & Europol, 2024). This highlights a fundamental flaw in legal systems designed for the physical world, where the identity of the perpetrator is evident, but in the digital sphere such barriers do not exist and traces are easily erased. Although they provide the foundation for combating cybercrime, legal systems have major limitations that require fresh ideas and adaptation to modern technical issues.

3. Challenges in the fight against cybercrime

Cybercrime is one of the most complex threats of our time, and legal systems globally encounter several challenges in attempting to combat it. Another fact, at this time, is that while technology continues to advance rapidly, legislation and law enforcement mechanisms are usually years behind and the criminals work in the shadows with the greatest ease (Marković & Zirojević, 2024). An examination of these difficulties shows deep-seated structural and practical challenges, from jurisdictional complications to a lack of technical expertise, that collectively hinder the effective fight against this global menace.

One of the most serious hurdles in fighting cybercrime is jurisdiction. Cyber attacks are not limited by geography – the actor in one country, the infrastructure used for the attack in a second, the victim in a third. For instance, a Chinese hacker can hack the server of an American company using an intermediary server in Brazil, while the ransom for the ransomware should be paid via cryptocurrency through the Dubai stock exchange. What country has jurisdiction to investigate and prosecute this case? China because the hacker is located there? America, because the victim is on my side there? Brazil, because it was how its infrastructure was used? Or Dubai, since the money went there? These are not just hypothetical questions – we have sen in the Europol report that the majority of cyber attacks go unsolved for exactly these jurisdictional reasons (Eurojust & Europol, 2024). Hackers are signing up for VPNs, working on the dark web and making anonymous payments to cover their tracks, leaving judicial authorities in a stalemate over who has jurisdiction (more details in Zirojević & Ivanović, 2021).

Another major problem is the law becoming old. Many cybercrime laws were already written decades ago, long before the Internet enjoyed the status it enjoys today. One example can be from our country, Serbia, where the Law on Information Security was adopted in 2016, but this law and the Criminal Code have not been significantly updated in that context since then, which has led to provisions that do not reflect modern forms of cybercrime (forexample mass ransomware attacks, etc., as well as the misuse of artificial intelligence to create false identities). Other countries share the same fate – the US still utilizes the Computer Fraud and Abuse Act of 1986, vintage from an era when few owned computers and the Internet was fresh, to prosecute cybercriminals. Such legislation is generally not well equipped to tackle modern threats, likethe tracing ofotherwise untraceable bitcoin transactions or preventing attacks on critical infrastructure through advanced botnets.

We encounter another hurdle in the technological backwardness of judicial systems. Many police, prosecutors and courts lack the tools to monitor cyber attacks. Tracking fraud transactions, for instance, calls for specialized software and knowledge of blockchain technology yet that is not exactly the case in Serbia, the majority of police agencies there lack even fundamental resources for such a task. Police officers in Europe are not sufficiently trained to deal with large amounts of data in cybercrime investigations, and it can be said that they lag behind technology, which is why they have many problems in the field of digital forensics (Muncaster, 2025). The courts complicate things further – judges often don't have the technical skills to evaluate seemingly arcane evidence, like server logs or messages encrypted from the dark web.

Furthermore, there is tension between privacy and security (Domazet, Marković & Skakavac, 2024), complicating efforts to combat cybercrime. Regulations similar to GDPR in the E.U., while important to privacy (Mladenov, 2023), impose tight constraints on data collection and sharing, slowing investigations. For example, if the police want to obtain user data from a technology company, they must complete complex procedures to comply with the GDPR, giving criminals an opportunity to cover their tracks. Meanwhile, the likes of Apple and WhatsApp employ end-to-end encryption for their messages, enabling them not even to access user content, even when police demand it. This led to a worldwide debate – the British government fought in 2024 to start a campaign to outlaw end-to-end encryption, claiming it obstructed inquiries into cybercrime, but faced stiff resistance from privacy activists, who argued that this would infringe users' basic rights (Szóka & Boulton, 2025).

There aren't many experts in forensic science who have some knowledge of cybercrime, especially not in a place like Serbia, where salaries in the public sector are paltry and private companies can provide better working conditions.

Experts estimated four years ago that there will be a shortage of 3.5 million cyber professionals in 2025, three and a half times more than in 2013, which is staggering, but in judicial institutions, it is very glaring (Morgan, 2021). The police can't follow digital trails and the courts can't make sense of the evidence without specialists' help. Thus, they can find themselves in a position to absolve a hacker who steals data from a hospital system, a bank or even from government servers – simply because they do not have an expert who can confirm the authenticity of the digital evidence. These are challenges that remind us of the need of a transformational change of our legal system. Cybercrime is not merely a technical issue – it needs global cooperation, new

laws, investment in technology and training of specialists (Matijašević & Dragojlović, 2021). Without it, justice systems are always one step behind criminals who use the anonymity and speed afforded by the digital age to dodge justice.

4. Perspectives and solutions

It needs a holistic and synergistic approach towards cybercrime as existing laws systems have proved with limited success combatting this global threat. Indicators for the future related for example to international cooperation, modernization of laws, investments in technology and public education have been drawn on the basis of the analysis presented.

International cooperation is the starting point tackling cybercrime more effectively. The Budapest Convention is powerful but should be expanded to other countries, with key global actors like Russia and China missing from this framework and forming significant holes in the system. In this regard, the UN Agreement on Cybercrime (Council of Europe, 2025) can serve as an important enabler in this wider framework of cooperation. States should align their legislation and facilitate information sharing so that perpetrators can be swiftly tracked down and prosecuted, no matter where jurisdiction lies.

Equally important is the modernization of national laws. The two legal acts, the Law on Information Security and the Criminal Code, need to be harmonized with modern threats, such as ransomware attacks and cryptocurrency abuse. By way of example, provisions that would trace the anonymous cryptocurrency transactions would mean much more could be traced. Similarly, countries such as the US would have to reform archaic legislation such as the Computer Fraud Act of 1986, in order for such laws to include new types of cybercrime (Berris, 2020), including abuse of artificial intelligence.

Technological advances are no end of the answer to the backwardness of many law enformcements. Acquiring specialized digital trail tracing tools – like software for analyzing blockchains – would help police and courts to prosecute criminals more efficiently. Forensic experts need to be trained – estimates of the lack of 3.5 million cyber security experts are certainly worrying, and Serbia is particularly vulnerable in this regard. To address this gap, states need to invest in the education and employment of experts.

Public education is a major component of prevention. It helps reduce the number of victims, as exemplified by Internet safety campaigns – e.g. a good practice example is Estonia (Holm, 2025) – through the use of e-government

and training of citizens, this country has greatly decreased cybercrime. A similar approach could be followed in Serbia, where users' awareness of digital threats is still low.

Finally, the great news is that artificial intelligence is also being applied to detect and prevent cyberattacks. Artificial intelligence tools can recognize attack patterns and predict them, but there is also a risk of misuse, so additional guidelines are needed for their use. The answer to this lies in a level of global co-ordination, advancements in tech and education – and only then can we hope the law will be able to keep up with the cybercriminals.

5. Conclusion

Cybercrime in the digital age has emerged as a global scourge, a threat that legal systems around the world have had difficulty addressing, and this study identifies important challenges and potential avenues for reform. Based on the theoretic review of international and national legal framework it can be concluded that existing mechanisms (Budapest Convention, GDPR) provide a basis for cybercrime fighting, however, they are constrained by inconsistency of legal frameworks in relation of the countries and ways of modern technologies. Law on Information Security and the Criminal Code regulate the field in Serbia, but implementation is one step behind due to the absence of experts and technical capacity. Difficulties like jurisdictional complexity, technology lag, and privacy versus security also make an effective response difficult – Europol reported in 2024 that most cyber attacks go unresolved, primarily due to the anonymity facilitated by VPNs and the dark web.

It is necessary to take a holistic approach in order to combat cybercrime. The Budapest Convention should be expanded to include more countries, and countries like Russia and China should be included in global agreements. This will help promote international collaboration. National legislation must be modernized to deal with current threats like ransomware attacks and the use of cryptocurrencies. Educating the public, training forensic experts and providing specialized tools for the police and courts is the next step towards uncovering new digital clues. And privacy and security must be reconciled – lawmakers have to strike the balance between wanting to protect user data and enabling effective investigations. The future includes international treaties such as the UN Cybercrime Treaty and the application of artificial intelligence to detect and prvent attacks, but till then the cybercriminals are one step ahead of justice without global coordination and tech advances.

Marković M. Darko
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Marković Darija
Univerzitet RUDN, Pravni institut, Moskva, Rusija

KIBERNETSKI KRIMINAL I PRAVO – UPRAVLJANJE IZAZOVIMA I PERSPEKTIVAMA U DIGITALNOM DOBU

APSTRAKT: Kibernetski kriminal u digitalnom dobu se pojavio kao globalna pretnja koja izaziva pravne sisteme širom sveta sa višestrukim ograničenjima efikasnosti i primenljivosti. Istražujemo kako se ovi izazovi rešavaju u međunarodnim i nacionalnim pravnim okvirima, naglašavamo ključne prepreke i pružamo perspektive za unapređenje. U radu se pokušavaju sagledati postojeći pravni mehanizmi, uključujući Budimpeštansku konvenciju i GDPR i nacionalne zakone u Srbiji, kao i njihova prilagodljivost savremenoj tehnološkoj pretnji i mogućnostima za reformu. Ovo istraživanje je zasnovano na interdisciplinarnoj metodologiji, kombinujući teorijsku analizu međunarodnih i domaćih pravnih tekstova sa činjeničnim proučavanjem statističkih podataka i evidencije slučajeva. Praktični izazovi sprovođenja zakona se procenjuju kroz sistematsko raščlanjivanje relevantnih izvora, uključujući broj prijavljenih slučajeva sajber napada, izveštaje Interpola i Evropola u kojima se daju uvidi u određene slučajeve. Nalazi naglašavaju sistemske izazove, kao što su ograničenja u nadležnostima, neefikasni zakoni i nedostatak tehničkih kapaciteta, dok rešenja ukazuju na veću međunarodnu saradnju, modernizaciju zakona, ulaganje u tehnologiju i javno obrazovanje. Rad dolazi do zaključka da bi trebalo da postoje koordinisani međunarodni napori da se poboljša pravna otpornost na kibernetski kriminal, kako bi se prodrlo kroz sajber zidove koji štite kriminalce.

Ključne reči: *sajber kriminal, pravo, digitalno doba, jurisdikcija, međunarodna saradnja.*

References

1. Behera, S. K. (2024). The Facebook data breach and its consequences for consumer privacy and cybersecurity. *National Journal of Cyber Security Law*, *7*(1), pp. 1–6
2. Berris, P. G. (2020). *Cybercrime and the law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. Congressional Research Service. Downloaded 2025, March 14 from https://www.congress.gov/crs_external_products/R/PDF/R46536/R46536.3.pdf
3. Beveridge, C. (2023). Irish Data Protection Commissioner imposes a €1.2 billion fine on Meta Ireland. *BDO Global Portal*. Downloaded 2025, February 28 from https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/irish-data-protection-commissioner-imposes-a-1-2-billion-fine-on-meta-ireland
4. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
5. Council of Europe. (2024). *United Nations treaty on cybercrime agreed by the Ad Hoc Committee*. Council of Europe Portal. Downloaded 2025, March 15 from https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee
6. Council of Europe. (2001). *Convention on Cybercrime* (European Treaty Series No. 185). Budapest, Hungary. Downloaded 2025, March 15 from https://rm.coe.int/1680081561
7. Domazet, S., Marković, D. M., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveilance. *Pravo – teorija i praksa*, *41*(3), pp. 109–124. DOI:10.5937/ptp2403109D
8. Easterly, J., & Fanning, T. (2023). *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years*. CISA America's Cyber Defense Agency. Downloaded 2025, March 14 from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
9. eSentire. (2024). *Cybersecurity Ventures report on cybercrime*. eSentire. Downloaded 2025, March 5 from https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime
10. European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)* (Official Journal of the European Union, L 119/I of 4 May 2016). Downloaded 2025, February 28 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

11. Griffiths, C. (2025). *The latest 2025 ransomware statistics (updated January 2025)*. AAG. Downloaded 2025, March 5 from https://aag-it.com/the-latest-ransomware-statistics/
12. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecrutiy challenge and solutions under the climate of COVID-19 scoping review. *Journal of Medical Internet Research*, *23*(4), e21747. DOI: 10.2196/21747
13. Holm, P. (2025). *Estonia's bold approach to cyber security: A holistic model for Europe*. e-Estonia. Downloaded 2025, March 22 from https://e-estonia.com/estonias-cyber-security-model-for-europe/
14. Krivični zakonik [Criminal Code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 i 94/24
15. Marković, D. M., & Zirojević, M. (2024). Izazovi u regulisanju i identifikaciji deepfake sadržaja [Challenges in regulating and identifying deepfake content]. In: Počuča, M. (ed.), *XXI međunarodni naučni skup „Pravnički dani – Prof. dr Slavko Carić" Odgovori pravne nauke na izazove savremenog društva* [*XXI International Scientific Conference "Legal days – Prof. Slavko Carić, PhD" The responses of legal sciences to the challenges of modern society*] (pp. 679–692). Novi Sad: Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, DOI: 10.5937/PDSC24679M
16. Matijašević, J., & Dragojlović, J. (2021). Metodika otkrivanja krivičnih dela računarskog kriminaliteta [Methodology of detection of computer crime offenses]. *Kultura polisa*, *18*(2), pp. 51–63. DOI:10.51738/Kpolisa2021.18.2p.1.04
17. Mladenov, M. (2023). Human vs. Artificial intelligence – EU's legal response. *Pravo – teorija i praksa*, *40*(1), pp. 32–43. DOI:10.5937/ptp2300032M
18. Morgan, S. (2021). *Cybersecurity jobs report: 3.5 million unfilled positions in 2025*. Cybersecurity Ventures. Downloaded 2025, March 19 from https://cybersecurityventures.com/jobs-report-2021/
19. Muncaster, P. (2025). *European police: Data volumes and deletion hindering investigations*. Infosecurity Magazine. Downloaded 2025, February 28 from https://www.infosecurity-magazine.com/news/police-data-volumes-deletion/
20. Palatty, N. J. (2025). *How many cyber attacks per day: The latest stats and impacts in 2025*. Astra IT. Downloaded 2025, March 25 from https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/

21. Samsoerizal, A. D., Hidayat, E. R., & Sukendro, A. (2022). Analytical study of Indonesian cybersecurity lesson learned from Estonian Cyberattacks in 2007. *International Journal of Arts and Social Science*, *5*(2), pp. 31–36. https://www.ijassjournal.com/2022/V5I2/414659927.pdf
22. Szóka, B., & Boulton, S. (2025). *UK encryption crackdown imperils privacy, security & free speech*. Tech Policy Press. Downloaded 2025, March 15 from https://www.techpolicy.press/uk-encryption-crackdown-imperils-privacy-security-free-speech/
23. Zakon o informacionoj bezbednosti [Law on Information Security]. *Službeni glasnik RS*, br. 6/16, 94/17, 77/19
24. Zirojević, M., & Ivanović, Z. (2021). *Cyber law – Serbia.* Belgrade: The Institute of Comparative Law