STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2025. II. évfolyam 1. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés Csernák Krisztina (L'Harmattan) munkája
A nyomdai munkákat a Robinco Kft. végezte, felelős vezető Gembela Zsolt

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

TRENDS IN INVESTIGATING CYBERCRIME: LEGAL AND PRACTICAL CHALLENGES IN THE DIGITAL AGE

A KIBERBŰNÖZÉS NYOMOZÁSI TENDENCIÁI: JOGI ÉS GYAKORLATI KIHÍVÁSOK A DIGITÁLIS KORBAN

Francois Regis Nshimiyimana[1]

ABSZTRAKT ■ Ez a tanulmány a kibertámadások legújabb tendenciáit, valamint a nyomozók előtt álló jogi és gyakorlati kihívásokat vizsgálja a digitális korban. Elemzi az olyan kulcsfontosságú kérdéseket, mint az aluljelentés, az anonimitás, a joghatósági bonyodalmak és a kiberbűnözés határokon átnyúló jellege. A kutatás célja e kihívások értékelése, valamint jogi és nyomozati stratégiák kidolgozása a kiberbűnözés elleni fellépés hatékonyságának növelése érdekében.

Az eredmények azt mutatják, hogy a szabványosított jogi keretek hiánya, a digitális bizonyítékok gyűjtésének és hitelesítésének nehézségei, valamint a korlátozott nemzetközi együttműködés jelentős mértékben hátráltatják a hatékony kiberbűnözési nyomozásokat. Emellett a kiberbűnözők egyre kifinomultabb módszerei speciális szakértelmet és naprakész jogi eszközöket igényelnek. Ez a kutatás hozzájárul a kiberbűnözés szabályozásáról és nyomozásáról szóló folyamatos diskurzushoz. Gyakorlati ajánlásokat kínál a jogi keretek megerősítésére, a nyomozati képességek javítására, valamint a nemzetközi együttműködés fokozására a kiberbűnözés elleni küzdelemben.

Kulcsszavak: kiberbűnözés, nyomozás, joghatóság, digitális bizonyíték

ABSTRACT ■ This paper explores emerging trends in cybercrime and legal and practical challenges investigators face in the digital age. It examines key issues such as underreporting, anonymity, jurisdictional complexities the transnational nature of cybercrime. The study aims to assess these challenges and propose legal and investigative strategies to enhance the enforcement of cybercrime.

The findings indicate that the absence of standardized legal frameworks, challenges in collecting and authenticating digital evidence, and limited international cooperation significantly hinder effective cybercrime investigations. Furthermore, the growing sophistication of

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of Reformed Church in Hungary; researcher on electronic evidence in cybercrime; e-mail: regisnshimiye82@gmail.com; ORCID: https://orcid.org/0009-0001-4723-1485.

cybercriminal tactics necessitates specialized expertise and updated legal instruments. This research contributes to the ongoing discourse on cybercrime regulation and investigation. It provides practical recommendations to strengthen legal frameworks, improve investigative capabilities, and enhance international collaboration in combating cybercrime.

Keywords: cybercrime, investigation, jurisdiction, digital evidence

1. Introduction

In the digital age, cybercrime has evolved into a complex and pervasive threat transcending national borders, posing significant challenges to law enforcement agencies and legal systems worldwide.[2] As technology advances, so do cybercriminals' tactics, making traditional investigative methods increasingly inadequate.[3] The anonymity of online environments, jurisdictional complexities, and the transnational nature of cybercrime further complicate enforcement efforts.[4] Additionally, underreporting and the lack of standardized legal frameworks hinder effective legal responses, leaving gaps that cybercriminals exploit.

This paper explores emerging trends in cybercrime and the legal and practical obstacles investigators face in combating these offenses. It examines critical issues such as digital evidence collection, authentication challenges, and the role of international cooperation in cybercrime enforcement. By analyzing these factors, this study aims to assess the effectiveness of current legal and investigative approaches and propose strategies to enhance cybersecurity enforcement mechanisms.

This research contributes to the ongoing discourse on cybercrime regulation by offering practical recommendations to strengthen legal frameworks, improve investigative capabilities, and foster international collaboration. The findings provide valuable insights for policymakers, law enforcement agencies, and legal professionals striving to develop more robust responses to cyber threats in an increasingly digital world.

[2] David S. Wall: *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, Polity Press, 2024, https://www.researchgate.net/profile/David-Wall-7/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition/links/65c36f3179007454976a5420/Cybercrime-The-Transformation-of-Crime-in-the-Information-Age-2nd-edition.pdf (Accessed on February 8, 2025.).

[3] Ibid.

[4] Jan Kleijssen – Pierluigi Perri: *Cybercrime, Evidence and Territoriality: Issues and Options.* Council of Europe, 2017. https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98 (Accessed on February 7, 2025.).

'Background and importance of the study': The digital revolution has reshaped societal interactions, economic structures, and governance frameworks and facilitated the proliferation of cybercrime. As reliance on digital technologies grows, so do the vulnerabilities that cybercriminals exploit, ranging from financial fraud and data breaches to sophisticated cyberattacks on critical infrastructure. Cyber offenses' increasing complexity and transnational nature pose significant challenges to legal practitioners, law enforcement agencies, and policymakers. Traditional legal frameworks designed for territorial jurisdictions often struggle to adapt to crimes committed in cyberspace, where national borders are largely irrelevant.

In Cybercrime, the Transformation of Crime in the Information Age, David S. Wall highlights how the intersection of technology and criminal behavior necessitates reevaluating existing legal and investigative approaches.[5] Cybercriminals leverage anonymity, encryption, and decentralized networks to evade detection and prosecution, complicating electronic evidence collection, authentication, and admissibility.[6] Furthermore, jurisdictional conflicts and the lack of standardized international legal mechanisms hinder cross-border cooperation, allowing cyber offenders to exploit legal loopholes in different jurisdictions.[7]

The study's importance lies in its contribution to address these challenges by analyzing emerging trends in cybercrime and proposing legal and investigative strategies to enhance enforcement efforts. By examining key issues such as underreporting, evidentiary challenges, and jurisdictional limitations, this research provides actionable insights for legal practitioners, policymakers, and law enforcement agencies. It aligns with the ongoing efforts of international organizations, such as the Council of Europe's Budapest Convention on Cybercrime, to establish coherent legal frameworks and foster global cooperation in cybercrime regulation.[8]

This study is particularly relevant given the increasing sophistication of cyber threats and the urgent need for legal systems to adapt. It seeks to inform and support the development of robust policies that enhance investigative capabilities and protect fundamental rights in the digital space.

5 Ibid. 2.

6 Ibid. 4.

7 United Nations Office on Drugs and Crime: *Comprehensive Study on Cybercrime*, 2013, 89. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdft.

8 Council of Europe: *Convention on Cybercrime*. ETS No.185, 2001, Article 22. Available at: Council of Europe.

'Rapid evolution of cybercrime in the digital age and the necessity of effective investigative and legal responses': The rapid evolution of cybercrime in the digital age has fundamentally reshaped the threat landscape, with cybercriminals continuously adapting their methods to exploit emerging technologies.[9] Encrypted communication, decentralized platforms, and artificial intelligence have made cyber offenses more sophisticated, enabling perpetrators to operate anonymously and across multiple jurisdictions. As David S. Wall notes, the transformation of crime in the information age necessitates a shift in how legal systems conceptualize, investigate, and prosecute cyber offenses.[10] The borderless nature of cyberspace further complicates traditional law enforcement mechanisms, creating jurisdictional conflicts that often hinder international cooperation and prosecution efforts.[11] Without robust legal frameworks and investigative tools, cybercrime will continue to outpace regulatory and enforcement measures, posing a persistent challenge to global security and economic stability.

As societies increasingly rely on digital platforms for communication, financial transactions, and critical infrastructure management, the risks associated with cybercrime have intensified.[12] Data breaches, financial fraud, and ransomware attacks have demonstrated the vulnerabilities inherent in digital ecosystems, affecting individuals, businesses, and governments. Given the scale and impact of cyber threats, it is imperative to establish comprehensive legal and investigative responses that balance enforcement capabilities with fundamental rights protection.[13] Strengthening international cooperation, harmonizing legal standards, and enhancing digital forensic capabilities are crucial to mitigating the growing cybercrime threat. This study contributes to the broader discourse on cybercrime regulation and enforcement by addressing these pressing challenges and offering practical recommendations to fortify legal frameworks and investigative strategies in the digital age.

'Research problem and justification': The increasing complexity and transnational nature of cybercrime pose significant challenges for law enforcement

[9] Mthokozisi Hlatshwayo: *Cybersecurity in the Digital Space.* Wits Business School, 2023. Available at: https://www.researchgate.net/publication/375115830_CYBERSECURITY_IN_THE_DIGITAL_SPACE.

[10] Ibid. 2.

[11] Kristin M. Finklea: *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*. Congressional Research Service, 2013. Available at: https://sgp.fas.org/crs/misc/R41927.pdf.

[12] Yuchong Li – Qinghui Liu: A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments. *Energy Reports*, 2021 (7), 8176–8186. Available at: https://www.sciencedirect.com/science/article/pii/S2352484721007289.

[13] Ibid. 4.

and legal systems worldwide.[14] Cybercriminals exploit jurisdictional gaps, operate anonymously across multiple legal frameworks, and leverage sophisticated techniques that outpace traditional investigative methods. Despite international conventions like the Budapest Convention on Cybercrime, enforcement remains inconsistent due to varying national legislations, limited cross-border cooperation, and difficulties in collecting and authenticating digital evidence. The lack of a standardized global legal framework further complicates efforts to prosecute cybercriminals effectively.

This research is essential due to the growing reliance on digital platforms for personal, economic, and governmental activities, which increases vulnerabilities to cyber threats. As cybercrime becomes more advanced and globalized, existing legal and investigative mechanisms struggle to keep pace, leaving critical gaps in cybersecurity enforcement. Addressing these challenges requires comprehensive legal and investigative strategies, including improved digital evidence collection procedures, enhanced international cooperation, and updated legislative frameworks. This study strengthens cybercrime regulation and investigation by identifying weaknesses in current enforcement mechanisms and proposing practical solutions, a crucial step toward ensuring global cybersecurity resilience.

'Methodology': This study employs a qualitative approach, combining doctrinal legal analysis and comparative legal methodology to examine cybercrime enforcement globally. It analyzes international treaties, national laws, case law, and scholarly literature to assess legal frameworks and investigative challenges. A comparative analysis highlights differences in cybercrime enforcement across jurisdictions, focusing on jurisdictional conflicts, evidence authentication, and international cooperation. Additionally, case studies illustrate real-world enforcement challenges, while policy reports and expert opinions provide interdisciplinary insights. This approach comprehensively evaluates legal gaps and proposes practical solutions to enhance cybercrime investigation and regulation.

2. Emerging trends in cybercrime and their impact on investigations

The rapid evolution of technology has significantly transformed the landscape of cybercrime, presenting new challenges for law enforcement and legal systems worldwide.[15] As cybercriminals adopt increasingly sophisticated tactics,

[14] Roderic Broadhurst: Developments in the Global Law Enforcement of Cyber-Crime. *Policing: An International Journal*, 2006 (3), 408–433, https://doi.org/10.1108/13639510610684674.

[15] Ibid. 9.

traditional investigative methods often struggle to keep pace. Emerging trends such as the rise of ransomware, deepfake technology, cryptocurrency-related crimes, and AI-driven cyber threats have expanded the complexity and scope of cybercrime investigations.[16]

These developments complicate the identification and prosecution of offenders and expose gaps in legal frameworks and investigative capabilities. Jurisdictional challenges, encrypted communication channels, and the anonymous nature of cyber offenses further hinder effective law enforcement responses. This section examines the latest trends in cybercrime and analyzes their impact on digital investigations, highlighting key obstacles and proposing strategies to strengthen enforcement mechanisms.

2.1. Key Cybercrime trends

Cybercrime has evolved significantly in recent years, driven by technological advancements and societal behavior shifts. The following are some of the most critical trends shaping the cyber threat landscape:

2.1.1. The rise of ransomware attacks

Ransomware attacks have become increasingly sophisticated, targeting individuals, corporations, and critical infrastructure worldwide. Cybercriminals employ advanced encryption techniques to lock victims out of their systems, demanding substantial ransoms for decryption keys. A notable example is the Colonial Pipeline attack in 2021, where the DarkSide ransomware group disrupted fuel supply chains in the United States, leading to widespread shortages and economic impact. In response, the U.S. Department of Justice seized a significant portion of the ransom paid in cryptocurrency, highlighting the growing focus of law enforcement on such attacks.[17]

Recent cases such as the attack on the Costa Rican government in 2022 by the Conti ransomware group[18] and the 2023 MGM Resorts breach, which led to an

[16] Michael Waddington: Cybercrime Trends and Evolving Cyber Laws in 2025: A Forward-Looking Analysis. *Criminal Defense Lawyer*, 2024. Available at: https://www.linkedin.com/pulse/cybercrime-trends-evolving-cyber-laws-2025-analysis-waddington-tb95e/ (Accessed on February 7, 2025.).

[17] Jen Easterly: *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. CISA, 2023. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[18] Jason Firch: *Conti Costa Rica Ransomware Attack Explained*. PurpleSec, 2024. Available at: https://purplesec.us/breach-report/conti-ransomware-attack/.

estimated $100 million in losses, demonstrate the persistence of ransomware as a major cyber threat.[19] Courts and regulatory bodies are increasingly addressing these incidents, with the European Union tightening its cybersecurity directives to mitigate risks.[20]

2.1.2. The prevalence of phishing attacks

Phishing remains one of the most pervasive cyber threats, leveraging social engineering tactics to deceive individuals into divulging sensitive information.[21] Attackers increasingly employ spear phishing techniques, using tailored messages that exploit personal data from social media and breached databases.[22] A recent example occurred in 2023 when a large-scale phishing campaign targeted Microsoft 365 users, compromising thousands of business accounts globally.[23] Additionally, the United Kingdom's High Court ruled in Lloyd v. Google LLC (2021) that mass data breaches caused by deceptive cyber tactics could result in substantial compensation claims for affected users, reinforcing the need for stricter regulatory oversight.[24]

2.1.3. Cryptocurrency-related crimes

The rapid expansion of digital assets has led to a surge in cryptocurrency-related cybercrimes. Due to their pseudonymous nature, cryptocurrencies are frequently exploited for illicit activities, including money laundering, fraud, and ransomware payments.[25] One of the most significant cases involved the Bitfinex hack, where cybercriminals laundered approximately $4.5 billion in stolen cryptocurrency

[19] Casino giant MGM expects $100 million hit from hack that led to data breach, Reuters, October 5, 2023, 9:40 PM EDT. Available at: https://edition.cnn.com/2023/10/05/business/mgm-100-million-hit-data-breach/index.html.

[20] European Commission, Shaping Europe's Digital Future: Cybersecurity Policies, 2023. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

[21] Mike Miller: *Social Engineering Beyond Phishing: New Tactics and How to Combat Them*. 2025. Available at: https://www.auditboard.com/blog/social-engineering-beyond-phishing-new-tactics-and-how-to-combat-them/.

[22] Ibid.

[23] Microsoft 365 Phishing Attacks Surge, Compromising Business Accounts Worldwide, TechCrunch, March 2023.

[24] Lloyd (Respondent) v Google LLC (Appellant), UKSC/2019/0213. Available at: https://www.supremecourt.uk/cases/uksc-2019-0213.

[25] Homeland Security, Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies, 2022. Available at: https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf.

before their arrest in 2022.[26] Similarly, fraudulent Initial Coin Offerings (ICOs) continue to deceive investors, prompting regulatory agencies, including the U.S. Securities and Exchange Commission (SEC), to intensify crackdowns on fraudulent crypto schemes.[27] The European Court of Justice has also issued rulings clarifying the legal status of digital assets and their taxation to combat financial crimes.[28]

2.1.4. AI-Driven Cyberattacks

Artificial Intelligence (AI) is increasingly weaponized by cybercriminals to enhance the scale and efficiency of their attacks. AI-powered phishing schemes, automated vulnerability scans, and deepfake-driven fraud attempts have escalated frequently. In 2023, a high-profile case involved using AI-generated voice deepfakes in a financial scam that defrauded a multinational firm of $35 million.[29]

Conversely, AI is also being deployed in cybersecurity defense mechanisms to detect and mitigate threats in real time. Courts are beginning to address AI-related cybercrimes, with legislative efforts aimed at regulating AI's dual-use capabilities for both security and malicious purposes.[30]

2.1.5. The dark web and illicit transactions

The dark web remains a critical platform for cybercriminal activities, including drug trafficking, weapons sales, and stolen data transactions. While law enforcement agencies have successfully dismantled several major dark web marketplaces, such as Hydra Market, in 2022, new platforms quickly emerged to fill the void. One of the most recent developments is the rise of decentralized dark web markets utilizing blockchain technology to evade tracking. The takedown of Genesis Market in 2023, which facilitated the sale of compromised login

[26] United States v. Lichtenstein, Case No. 1:22-mj-00028 (D.D.C. 2022). Available at: https://www.govinfo.gov/content/pkg/FR-2024-12-06/pdf/2024-27982.pdf.

[27] SEC v. Ripple Labs Inc., Case No. 20-cv-10832 (S.D.N.Y. 2020). Available at: https://www.sec.gov/enforcement-litigation/whistleblower-program/notice-covered-actions/award-claim-2024-123.

[28] Skatteverket v. David Hedqvist, Case C-264/14, EU:C:2015:718. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-264/14.

[29] AI-Generated Voice Scams on the Rise, Deepfake Fraud Costs Multinational $35 Million, Forbes, July 2023. Available at: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/.

[30] Members of the Robotics and AI Law Society (RAILS), The European Commission's Proposal for an Artificial Intelligence Act-A Critical Assessment, 2021, 589–603. Available at: https://doi.org/10.3390/j4040043.

credentials, exemplifies ongoing enforcement efforts.[31] However, the dynamic nature of dark web markets continues to challenge authorities.

In summary, the evolution of cybercrime necessitates continuous adaptation in legal frameworks and law enforcement strategies. The surge in ransomware, phishing, cryptocurrency fraud, AI-driven attacks, and dark web activities underscores the critical need for enhanced regulatory oversight and international cooperation. Judicial decisions and policy developments worldwide are increasingly shaping the legal landscape to address these emerging threats, reinforcing cybersecurity as a priority in digital governance.

2.2. Impact on investigation

The rapid evolution of cybercrime presents significant challenges for law enforcement and forensic investigators, necessitating constant adaptation of investigative techniques. Cybercriminals are becoming increasingly sophisticated, employing advanced evasion tactics and leveraging emerging technologies to conceal their activities.[32] In response, digital forensic methods have evolved to incorporate AI-driven analysis, blockchain tracing, and cloud forensics.[33] However, the detection and tracking of cyber offenses remain complex due to encrypted communications, cross-border legal barriers, and the anonymity of illicit online markets. These factors collectively demand a more coordinated and technologically advanced approach to cybercrime investigations.

2.2.1. Increased sophistication of cyber criminals

Cybercriminals are employing increasingly advanced techniques to evade detection and compromise digital systems. The rise of artificial intelligence (AI)-driven attacks, ransomware-as-a-service (RaaS), and deepfake technology has made cyber offenses more complex than ever before. Criminals leverage encrypted communication channels, blockchain technology, and anonymization tools such as The Onion Router (TOR) to obscure their identities and operations.[34]

[31] FBI and International Partners Dismantle Genesis Market, U.S. Department of Justice, 2023. Available at: https://www.justice.gov/archives/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.

[32] E-SPIN, AI-Powered Cybercriminals Rising, Evolution, Tactics, and Defense Strategies Against Advanced Digital Threats, Global Themes and Feature Topics, 2024. Available at: https://www.e-spincorp.com/ai-cybercriminals-evolution-tactics-defense-strategies/.

[33] Ibid.

[34] Europol: Internet Organised Crime Threat Assessment (IOCTA) 2022, European Cybercrime Centre (EC3), 2022. Available at: https://www.europol.europa.eu/cybercrime.

This sophistication poses significant challenges for law enforcement agencies, requiring them to adapt their investigative methodologies continuously.

2.2.2. Evolution of digital forensic techniques

To counter advanced cyber threats, digital forensic techniques have evolved to include artificial intelligence, machine learning, and automation in evidence analysis. Investigators now utilize advanced methods such as volatile memory analysis, cloud forensics, and blockchain forensics to uncover digital footprints.[35] However, the rapid development of technology creates a constant need for updated tools and methodologies, as traditional forensic approaches may become obsolete when confronted with modern cyber threats. The increasing reliance on cloud storage and remote computing further complicates evidence retrieval and chain-of-custody considerations.[36]

2.2.3. Challenges in detecting and tracking cyber offenses

Cybercrime investigations are hindered by jurisdictional complexities, encrypted communications, and the use of cryptocurrencies for illicit transactions. Unlike traditional crimes, cyber offenses often involve perpetrators operating across multiple legal jurisdictions, making international cooperation essential but challenging.[37] The dark web continues as a hub for criminal enterprises, where illicit goods, hacking tools, and stolen data are traded anonymously. Law enforcement agencies face difficulties penetrating such networks without violating legal and ethical boundaries.[38] Moreover, the high volume of cyber incidents strains forensic teams, requiring efficient prioritization and resource allocation to manage cyber threats effectively.

In summary, as cybercrime evolves, investigative techniques must advance in tandem. Law enforcement agencies require specialized training, enhanced collaboration mechanisms, and access to cutting-edge forensic tools to combat

[35] Brett Shavers: *Placing the Suspect Behind the Keyboard. Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. Waltham, Syngress, 2013, 87. Available at: https://vdoc.pub/documents/placing-the-suspect-behind-the-keyboard-using-digital-forensics-and-investigative-techniques-to-identify-cybercrime-suspects-a1slo54kbcq0.

[36] Marcus K. Rogers: Recent Advances in Digital Forensics. *Journal of Digital Investigation*, 2015 (2), 102–117.

[37] Council of Europe, Budapest Convention on Cybercrime, ETS No. 185, 2001. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[38] Michael McGuire: *Into the Web of Profit. The Darknet and its Facilitating Role in Cybercrime.* University of Surrey, 2019. Available at: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf.

cyber threats effectively. Addressing jurisdictional and technological challenges remains a key priority in ensuring successful cybercrime investigations.

2.3. Case studies and statistical evidence

The study of cybercrime requires a data-driven approach, combining case studies and statistical evidence to understand emerging threats, enforcement challenges, and legal responses. Recent cybersecurity reports highlight evolving cybercrime trends, shifting ransomware tactics, AI-driven attacks, and supply chain vulnerabilities. At the same time, legal precedents and enforcement actions demonstrate the ongoing struggle between cybercriminals and law enforcement agencies, shaping policy and regulatory frameworks. Analyzing these trends and legal responses gives a clearer picture of how cyber threats evolve and how legal systems adapt to counter them effectively.

2.3.1. Analysis of recent cybercrime trends based on cybersecurity reports

Recent analyses of cybercrime trends reveal a dynamic and evolving threat landscape, necessitating adaptive legal and enforcement strategies. In 2024, despite numerous high-profile attacks, ransomware payments experienced a significant decline. According to Chainalysis, ransomware payments dropped by 35%, totaling $814 million, compared to $1.25 billion in 2023.[39] This decline is attributed to successful law enforcement actions against significant ransomware groups and increased global awareness, leading to improved defenses. However, experts caution that ransomware trends are volatile, and sustained investment in cybersecurity remains essential.

Conversely, the World Economic Forum's Global Cybersecurity Outlook 2025 highlights a rise in cyber threats, exacerbated by geopolitical tensions and the complexity of supply chains.[40] The report emphasizes that sectors such as healthcare, financial services, and energy are particularly vulnerable, with artificial intelligence expanding cybercriminals' attack surface. Despite heightened awareness, a sense of complacency persists among companies, underscoring the need for proactive security measures.

[39] Chainalysis 2024, Ransomware Payments Decline by 35%, *Cybercrime Report*, 2025. Available at: https://www.wired.com/story/2024-ransomware-payments-fall-chainalysis.

[40] World Economic Forum: Global Cybersecurity Outlook 2025, Available at: https://www.reuters.com/sustainability/sustainable-finance-reporting/esg-watch-companies-complacent-about-cybercrime.

2.3.2. Legal precedents and enforcement responses

Legal frameworks and enforcement actions have evolved to address the complexities of cybercrime. Notably, law enforcement agencies' takedown of prominent ransomware groups like LockBit and BlackCat/ALPHV has disrupted cybercriminal operations, contributing to the decline in ransomware payments.[41] These actions demonstrate the effectiveness of coordinated international efforts in combating cyber threats. In the legal arena, cases such as United States v. Microsoft Corp. (2018) have set significant precedents regarding government access to data stored overseas.[42] In this case, the U.S. Supreme Court's ruling reaffirmed the importance of international legal principles and sovereignty in cyberspace, influencing subsequent legislation and enforcement strategies.

Furthermore, cybercriminals' increasing use of artificial intelligence has prompted legislative bodies to consider new regulations. The European Union's proposed Artificial Intelligence Act aims to address the dual-use nature of AI technologies, balancing innovation with security concerns.[43] This reflects a proactive approach to emerging cyber threats, emphasizing the need for adaptive legal frameworks. These developments underscore the critical role of robust legal frameworks and proactive enforcement in mitigating cyber threats. Continuous adaptation and international collaboration remain essential to address the evolving cybercrime landscape effectively.

3. Legal and jurisdictional challenges in addressing transnational cybercrime

The rise of transnational cybercrime presents significant legal and jurisdictional challenges for law enforcement agencies and judicial systems worldwide. As cybercriminal activities increasingly operate across multiple jurisdictions, traditional legal frameworks struggle to keep pace with the complexities of digital crimes. The absence of a universally harmonized legal approach and varying national regulations complicate international cooperation and enforcement

[41] The Guardian, Global Ransomware Payments Plunge by a Third Amid Crackdown, February 2025. Available at: https://www.theguardian.com/technology/2025/feb/05/global-ransomware-payments-plunge-by-a-third-amid-crackdown.

[42] Lawctopus, Recent Developments in Cybersecurity Law: Challenges and Opportunities, December 2024. Available at: https://www.lawctopus.com/academike/recent-developments-in-cybersecurity-law.

[43] European Commission, Proposal for an Artificial Intelligence Act, 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

efforts.[44] This section examines the primary legal and jurisdictional difficulties in addressing cybercrime across borders, focusing on the global nature of cyber offenses, jurisdictional conflicts, and the effectiveness of international legal instruments in combating these threats.

3.1. Cybercrime as a global challenge

Cybercrime has become an increasingly pervasive issue in the digital era, transcending national borders and challenging traditional legal frameworks. As technological advancements facilitate cross-border interactions, cybercriminals exploit jurisdictional gaps to engage in illicit activities ranging from financial fraud to cyberterrorism.[45] The absence of a harmonized global legal framework exacerbates enforcement difficulties, leaving individual states struggling to address cyber threats effectively. Despite various national efforts, discrepancies in legal definitions, procedural laws, and investigative capacities hinder the uniform prosecution of cyber offenses.

3.2. Jurisdictional complexities

One of the fundamental legal obstacles in combating transnational cybercrime is the issue of jurisdiction. Cyber offenses often involve multiple legal systems, so conflicts arise in determining which nation has the authority to investigate, prosecute, and adjudicate cases. Jurisdictional claims may overlap, mainly when cyberattacks originate from one country, target victims in another, and involve servers in third-party states.[46] Such complexities often lead to legal conflicts and impede practical law enforcement cooperation.

[44] European Union: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 12 July 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

[45] Nakul R. Padalkar: *Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Financial Flows.* Graduate School of Arts and Sciences & McDonough School of Business, Georgetown University, 2024. 4-13.

[46] Cybercrime and International Law, Jurisdictional Challenges and Enforcement Mechanisms. *African Journal of Biomedical Research*, 2024 (3). Available at: https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/2101?articlesBySimilarityPage=11.

Mutual Legal Assistance (MLA) treaties serve as a key mechanism for international collaboration in cybercrime investigations. However, traditional MLA processes are often slow and bureaucratic, rendering them ineffective in responding to the rapidly evolving nature of cyber threats.[47] Moreover, differences in national laws regarding data protection and electronic evidence further complicate cooperation between states. Extradition challenges also arise due to discrepancies in cybercrime legislation, as certain offenses may not be recognized as extraditable crimes in all jurisdictions.[48]

3.3. International legal frameworks and agreements

The international community has taken steps to address cybercrime through various legal instruments and cooperative mechanisms. The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, remains the most comprehensive and widely ratified treaty in this domain. It provides a framework for criminalizing cyber offenses, enhancing procedural laws, and fostering international cooperation in cybercrime investigations.[49] However, its effectiveness is limited by the non-ratification of key cyber powers such as China and Russia, which advocate for alternative frameworks.[50]

Beyond the Budapest Convention, international law enforcement agencies play a crucial role in transnational cybercrime mitigation. Organizations such as INTERPOL and EUROPOL facilitate cross-border investigations, intelligence sharing, and capacity building for national agencies. Despite these efforts, enforcement challenges persist due to differences in national laws, resource disparities, and the reluctance of some states to cooperate fully in cyber investigations.[51]

Additionally, emerging cyber threats necessitate continuous updates to existing legal frameworks. The introduction of new protocols to the Budapest Convention, as well as regional agreements like the African Union's Malabo Convention,

47 Anna-Maria Osula: *Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data*, 2015. Available at: https://ccdcoe.org/uploads/2018/10/Research_A-M.Osula_2015.pdf.

48 Ibid.

49 Council of Europe, Convention on Cybercrime, Budapest, 23 November 2001, European Treaty Series - No. 185, https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

50 Ibid.

51 Interpol, National Cybercrime Strategy Guidebook, April 2021. Available at: file:///C:/Users/mn%20Technology%20Group/Downloads/Cyber_Strategy_Guidebook.pdf.

highlights ongoing efforts to strengthen global cyber governance. However, achieving comprehensive international cooperation requires greater alignment of domestic laws, streamlined legal assistance mechanisms, and enhanced technical capacities among states.[52]

4. Anonymity and digital evidence in cybercrime investigations

In the digital age, anonymity plays a significant role in committing cybercrimes, enabling perpetrators to hide their identities and evade detection. The anonymity afforded by various technologies has given rise to new challenges in cybercrime investigations, especially concerning collecting and validating digital evidence.[53] This section explores the role of anonymity in cybercrime and the intricate issues associated with digital evidence in investigations.

4.1. The role of anonymity in cybercrime

Anonymity has become crucial in enabling cybercriminals to operate with relative impunity. Among the tools used to obscure identity are Virtual Private Networks (VPNs), Tor networks, and cryptocurrency mixing services, each playing a distinctive role in masking the perpetrators' digital footprints.[54]

Use of VPNs, Tor Networks, and Cryptocurrency Mixing Services: VPNs and Tor networks are commonly employed by cybercriminals to mask their IP addresses, making it harder for investigators to trace their geographical location or the origin of criminal activities. The Tor network, for instance, provides access to the "dark web", where illicit transactions and discussions often occur, further complicating the law enforcement task. Additionally, cryptocurrency mixing services, which obscure the transaction history of digital currencies like Bitcoin, complicate the process of tracking illegal financial transactions,

[52] African Union, Malabo Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[53] Benjamin Aziz: A Framework for Digital Forensics and Investigations. *International Journal of Digital Crime and Forensics*, 2015 (2), 1-22. DOI: 10.4018/jdcf.2013040101.

[54] Alicja Hagopian: *International Perspectives on Tor and the Dark Web: Guidance for Policymakers. MSc Thesis*. King's College London, 2021. DOI: 10.13140/RG.2.2.31869.23527.

allowing criminals to launder proceeds from cybercrimes such as ransomware attacks or fraud.[55]

Challenges in attributing Cyber offenses to perpetrators: These anonymizing technologies create significant challenges in attributing cyber offenses to specific individuals. Law enforcement agencies must rely on sophisticated investigative techniques, including the analysis of digital footprints, network traffic analysis, and collaboration with international counterparts, to overcome these hurdles.[56] However, due to the decentralized and often anonymous nature of online criminal behavior, it is difficult to pinpoint the exact location, identity, or even the intentions of the perpetrators involved in cybercrime.

4.2. Digital evidence in cybercrime investigations

Digital evidence has become indispensable in prosecuting cybercrimes, but its collection and use are complex.[57]

Importance of digital forensics in cybercrime cases: Digital forensics is critical in ensuring that electronic evidence is recovered, analyzed, and presented legally. It plays an essential role in tracing the origins of cybercrimes, reconstructing the timeline of events, identifying the tools and methods used by perpetrators, and establishing links between suspects and illegal activities. Forensic investigators use specialized tools and techniques to examine digital devices such as computers, mobile phones, and servers, uncovering crucial evidence that might otherwise remain hidden.[58]

Challenges in collecting, preserving, and authenticating electronic evidence: One of the foremost challenges in digital forensics is the proper collection and preservation of electronic evidence. Given the transient nature of digital data, evidence must be preserved in its original state to avoid tampering or data loss. This can be incredibly challenging when dealing with cloud-based systems

[55] Rosenblum Allen Law Firm, Cryptocurrency Asset Tracing in Las Vegas Criminal Cases, 2021, https://www.rosenblumlawlv.com/bitcoin-forensics/.

[56] Sanjay Goel – Brian Nussbaum: *Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. IEEE Open Journal of the Communications Society,* 2021 (2), 1082-1093. DOI: 10.1109/OJCOMS.2021.3074591, License CC BY 4.0.

[57] Matthew Ogunbukola: The Critical Role of Digital Forensics in the Modern Information Era (June 2024). Available at: https://www.researchgate.net/publication/381143019_The_Critical_Role_of_Digital_Forensics_in_the_Modern_Information_Era.

[58] Andre Slonopas: What Is Digital Forensics? A Closer Examination of the Field. *Information Technology Blog. American Public University*, March 22, 2024. Available at: https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/.

or encrypted files. Furthermore, authenticating digital evidence to ensure its reliability and integrity in court presents additional challenges, mainly when dealing with sophisticated cybercrimes that may involve multiple jurisdictions and rapidly evolving technology.[59]

4.3. Legal admissibility of digital evidence

The admissibility of digital evidence is a significant issue in cybercrime investigations, as courts require that evidence meet specific legal standards for it to be used in legal proceedings.

Comparative analysis of standards in Rwanda, EU, and international conventions: Legal systems worldwide have developed varying standards for the admissibility of digital evidence. In Rwanda, the use of electronic evidence in criminal proceedings is governed by the law on electronic transactions[60], cybercrime[61], and other related statutes. Comparatively, the European Union has developed robust legal frameworks, such as the General Data Protection Regulation (GDPR) and the E-Privacy Directive, which address both the protection of data and the admissibility of digital evidence in criminal trials. International conventions, such as the Budapest Convention on Cybercrime, provide guidelines for the collection and cross-border exchange of digital evidence, though variations in national laws complicate international cooperation.

Chain of custody and evidentiary integrity issues: The chain of custody is critical in ensuring that digital evidence remains unaltered and legally admissible. Maintaining a proper chain of custody in cybercrime investigations is particularly difficult due to the ease with which digital data can be copied or altered. Investigators must document each step in handling digital evidence, from its seizure to its analysis and presentation in court, to prove that it has not been tampered with.[62] Failure to maintain a proper chain of custody can

[59] Renato Fazzone: Digital Forensics Fundamentals: Successful Preservation of Evidence. *FTI Technology Blog*, 2024. Available at: https://www.ftitechnology.com/resources/blog/digital-forensics-fundamentals-successful-preservation-of-evidence.

[60] Law No.18/2010 of 12/05/2010 *relating to electronic messages, Electronic Signatures, and Electronic Transactions*, published in the Official Gazette No. 20 on 17/05/2010.

[61] Law No. 60/2018 of 22/8/2018 *on the Prevention and Punishment of Cyber Crimes*. Official Gazette No. Special of 25/09/2018.

[62] Mohamed Ali et al.: A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. *Symmetry,* 2022 (2), 334. https://doi.org/10.3390/sym14020334.

result in evidence being ruled inadmissible, undermining the effectiveness of the investigation.

5. The need for specialized investigative expertise in handling cybercrimes

The rapid evolution of digital technologies has given rise to complex cybercrimes, necessitating specialized investigative expertise within law enforcement agencies. The global increase in cyber threats, including ransomware attacks, financial fraud, and cyber-enabled human trafficking, has underscored the need for well-trained cybercrime investigators and digital forensics experts. These professionals are essential in identifying, collecting, analyzing, and preserving electronic evidence in compliance with legal standards.

5.1. Growing demand for cybercrime investigators and digital forensics experts

Despite the growing prevalence of cybercrimes, many law enforcement agencies face a significant shortage of skilled digital forensics experts. A 2023 study by Europol found that over 60% of European law enforcement agencies lack sufficient personnel with expertise in digital forensics and cybercrime investigations.[63] The shortage has resulted in case backlogs and prolonged investigation timelines, ultimately affecting the administration of justice. The 2021 'United States v. Sullivan case', where Uber's former Chief Security Officer was convicted for covering up a data breach, highlights the complexity of digital investigations and the necessity of specialized knowledge to prosecute cyber-related offenses effectively.[64]

Given the dynamic nature of cybercrime methodologies, continuous training, and capacity-building initiatives are crucial for law enforcement agencies.[65] The Budapest Convention on Cybercrime emphasizes the need for international

[63] Europol, Consolidated Annual Activity Report, June 18, 2024. Avialable at: https://www.europarl.europa.eu/cmsdata/286518/Europol%20CAAR%202023.pdf.

[64] United States v. Sullivan, No. 3:20-cr-00337-WHO (N.D. Cal. 2021). Available at: https://casetext.com/case/united-states-v-sullivan-301.

[65] Patryk Pawlak – Panagiota-Nayia Barmpaliou: Politics of Cybersecurity Capacity Building. Conundrum and Opportunity. *Journal of Cyber Policy*, 2017 (1), 123–144. https://doi.org/10.1080/23738871.2017.1294610.

cooperation and training programs to enhance investigative capabilities. Countries such as Singapore and Germany have established dedicated cybercrime training centers that offer advanced courses on digital evidence handling, blockchain analysis, and AI-driven cyber threat detection.[66] These initiatives ensure that law enforcement personnel remain adept at tackling emerging cyber threats.

5.2. Role of cybercrime units and public-private partnerships

Several nations have developed specialized cybercrime units to enhance investigative efficiency. The UK's National Cyber Crime Unit (NCCU) and the FBI's Cyber Division are notable examples of agencies that utilize cutting-edge technology and interdisciplinary teams to combat cyber threats. A recent success story includes the FBI's Operation Duck Hunt (2023), which dismantled the Qakbot malware network, a sophisticated cybercriminal infrastructure for ransomware and financial fraud.[67] Public-private partnerships play a vital role in combating cybercrimes. Law enforcement agencies frequently collaborate with cybersecurity firms such as Mandiant and CrowdStrike to leverage threat intelligence and forensic tools. Additionally, academic institutions contribute by developing advanced digital forensics methodologies. The partnership between INTERPOL and Kaspersky in 2022 led to identifying and mitigating a global ransomware network, demonstrating the effectiveness of such collaborations.[68]

5.2.1. Challenges in law enforcement training

The primary challenges in cybercrime investigations are the gap between legal frameworks and technological advancements. Many prosecutors and judges lack the technical knowledge to assess the admissibility of digital evidence, leading to inconsistencies in case outcomes.[69] The case of R v. Smith (2022), where a UK court dismissed key digital evidence due to improper chain of custody

66 Ibid.

67 International Investigation Disrupts the World's Most Harmful Cyber Crime Group, National Crime Agency, 2024. Available at: https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group.

68 United Nations Office on Drugs and Crime, Public-Private Partnerships on Cybercrime: Regional Perspective on Best Practices, Challenges, and Opportunities from the Americas, Africa, and Asia, 2024. Available at: https://www.unodc.org/documents/NGO/PDF/CSU-CyberCrime-240807-WEB.pdf.

69 Christa M. Miller: A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point. *Forensic Science International: Synergy*, 2023 (6), 100296. Available at: https://www.sciencedirect.com/science/article/pii/S2589871X2200081X.

procedures, underscores the need for comprehensive legal-technical training for all stakeholders in the criminal justice system.

5.2.2. Resource constraints and limited technological capabilities

Budget limitations often prevent law enforcement agencies from acquiring state-of-the-art forensic tools like artificial intelligence-driven analytics and blockchain forensic software. Developing nations, in particular, struggle with outdated infrastructure, making it challenging to track cybercriminals effectively. The African Cybercrime Response Centre (ACRC), launched in 2023, aims to address these disparities by providing digital forensics resources and training programs to under-resourced law enforcement agencies across the continent.[70]

In summary, the growing complexity of cybercrime demands a concerted effort to enhance investigative expertise through specialized training, public-private collaboration, and investment in forensic technology. Strengthening these areas will ensure law enforcement agencies are adequately equipped to combat cyber threats and uphold digital justice.

6. Strengthening legal frameworks and enhancing international cooperation

The increasing complexity of cybercrime necessitates a robust and adaptive legal framework, both at the national and international levels.[71] Effective responses require comprehensive domestic legislation and enhanced international cooperation to address jurisdictional challenges and facilitate the prosecution of cybercriminals. However, significant gaps persist in existing cybercrime laws, and global collaboration remains inconsistent, hampering the effective enforcement of legal measures. This section explores the deficiencies in current legal frameworks, underscores the necessity of stronger international cooperation, and proposes reforms to align legislation with evolving cyber threats.

[70] Africa Cyber Programme, Protecting the Most Vulnerable in Africa from Cyber Threats – Project Summaries, HM Government, Final Report, 22 September 2023. Available at: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2023/12/africa-cyber-programme.pdf.

[71] Olukunle Oladipupo Amoo: *The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System*. *World Journal of Advanced Research and Reviews*, 2024 (2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438.

6.1. Inconsistencies in National legislation

The major challenge in combating cybercrime is the lack of harmonization among national legal frameworks. Many jurisdictions have outdated or insufficient laws that fail to address emerging threats, such as ransomware, deepfake fraud, and AI-driven cyberattacks. The disparities in legal definitions and penalties for cyber offenses create safe havens for cybercriminals who exploit weak regulatory environments.[72] For example, while some countries impose stringent penalties for unauthorized access to computer systems, others treat it as a minor offense with minimal legal consequences. Such inconsistencies not only weaken enforcement but also hinder cross-border investigations and prosecutions.

6.2. The need for standardized regulations for digital evidence

Standardized regulations governing digital evidence collection, preservation, and admissibility are absent.[73] Given the transient and volatile nature of digital data, inconsistencies in evidentiary standards across jurisdictions compromise the effectiveness of cybercrime investigations. In some cases, improperly collected digital evidence has been dismissed in court, undermining prosecution efforts. Establishing clear and uniform guidelines for handling electronic evidence is essential to ensuring its integrity and admissibility in legal proceedings.

6.3. Enhancing international collaboration

Cybercrime is inherently transnational, necessitating international treaties and agreements to facilitate cooperation among states. The Budapest Convention on Cybercrime, adopted by the Council of Europe, remains the most comprehensive international treaty addressing cybercrime and electronic evidence.[74] However, many countries, particularly in Africa and Asia, have yet to accede to the

[72] Eurojust and Europol, Common Challenges in Combating Cybercrime, June 2019, Joint report, Europol and Eurojust Public Information. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf.

[73] Glen Dario Rodriguez – Fernando Molina-Granja: The Preservation of Digital Evidence and Its Admissibility in the Court. *International Journal of Electronic Security and Digital Forensics*, 2017 (1), 3-19. Available at: https://www.researchgate.net/publication/312665626_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court.

[74] Council of Europe, The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Convention, limiting its global reach.[75] To strengthen international collaboration, diplomatic engagements should prioritize the ratification of existing cybercrime treaties while promoting the development of new agreements tailored to emerging threats.[76] Additionally, bilateral and multilateral agreements can streamline processes such as extradition and mutual legal assistance, essential for prosecuting cybercriminals operating across borders.

6.4. Improving intelligence sharing among law enforcement agencies

States' reluctance to share intelligence hinders effective law enforcement collaboration due to concerns over sovereignty, privacy, and cybersecurity risks.[77] Establishing secure and legally binding mechanisms for information exchange is crucial to overcoming these challenges. The INTERPOL Cybercrime Directorate and the Europol European Cybercrime Centre (EC3) provide valuable models for fostering international intelligence sharing and capacity-building initiatives. Regional cooperation frameworks, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), also critically strengthen cross-border law enforcement efforts. However, practical implementation remains slow due to capacity constraints and a lack of political will.

6.5. Recommendations for updating outdated laws

Given the rapid evolution of cyber threats, legal frameworks must be continuously updated to remain effective. In this regard, Governments should:

Enact comprehensive cybercrime legislation that aligns with international best practices.

Clearly define cyber offenses and prescribe proportionate penalties.

[75] Ibid.

[76] United Nations Office on Drugs and Crime, UN General Assembly Adopts Landmark Convention on Cybercrime, press release, December 24, 2024. Available at: https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

[77] Pieter Matsaung – David Tubatsi Masiloane: The Role of Cyber Intelligence in Policing Cybercrime in South Africa: Insights from Law Enforcement Officers. *South African Journal of Criminal Justice*, published online November 6, 2024. Available at: https://www.tandfonline.com/doi/full/10.1080/10246029.2024.2421225.

Strengthen procedural laws to facilitate the collection and admissibility of digital evidence.

Implement mandatory cybersecurity reporting requirements for critical sectors like finance and healthcare.

Additionally, public-private partnerships should be encouraged to develop legal frameworks that address the unique challenges posed by emerging technologies such as blockchain and artificial intelligence.

7. Conclusion

Cybercrime investigation in the digital age presents a multifaceted challenge that requires a dynamic and adaptive legal and investigative framework. This paper has examined the emerging trends in cybercrime, highlighting the increasing sophistication of cybercriminal tactics and their impact on investigative processes. The study has also addressed transnational cybercrime's legal and jurisdictional complexities, emphasizing the need for enhanced international cooperation and harmonized legal frameworks. Furthermore, the discussion on anonymity and digital evidence has underscored the importance of developing robust evidence collection, authentication, and admissibility mechanisms. Finally, the necessity of specialized expertise in cybercrime investigations has been explored, stressing the urgency for continuous capacity-building initiatives for law enforcement and judicial authorities.

The findings reveal that the lack of standardized legal approaches, jurisdictional limitations, and the challenges posed by anonymity significantly hinder effective cybercrime investigations. Additionally, the rapid evolution of cyber threats demands continuous legal reforms and specialized investigative capabilities to counter emerging risks. To address these issues, this paper proposes strengthening international collaboration through mutual legal assistance agreements, fostering technological advancements in digital forensics, and enhancing the training of legal and investigative professionals to tackle cybercrime more efficiently.

As a personal contribution, this research offers a comprehensive analysis of current investigative challenges and proposes pragmatic solutions to bridge existing legal and procedural gaps. By integrating theoretical insights with practical considerations, the study contributes to the broader discourse on cybercrime regulation and enforcement, providing valuable recommendations for policymakers, legal professionals, and law enforcement agencies. It advocates for a forward-looking approach that prioritizes adaptability, cooperation, and expertise in combating cybercrime in an increasingly digitalized world.

Ultimately, the effectiveness of cybercrime investigations hinges on the ability of legal systems to evolve in response to technological advancements. This paper serves as a call to action for legislators, law enforcement agencies, and international bodies to adopt innovative and coordinated strategies to safeguard digital ecosystems and ensure justice in the face of evolving cyber threats.

Bibliography

African Union, Malabo Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Anna-Maria Osula: *Mutual Legal Assistance & Other Mechanisms for Accessing Extra-territorially Located Data*, 2015. Available at: https://ccdcoe.org/uploads/2018/10/Research_A-M.Osula_2015.pdf

Brett Shavers: *Placing the Suspect Behind the Keyboard. Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. Waltham, Syngress, 2013, 87. Available at: https://vdoc.pub/documents/placing-the-suspect-behind-the-keyboard-using-digital-forensics-and-investigative-techniques-to-identify-cybercrime-suspects-a1slo54kbcq0

Chainalysis 2024, Ransomware Payments Decline by 35%, *Cybercrime Report*, 2025. Available at: https://www.wired.com/story/2024-ransomware-payments-fall-chainalysis.

Christa M. Miller: A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point. *Forensic Science International: Synergy*, 2023 (6), 100296. Available at: https://www.sciencedirect.com/science/article/pii/S2589871X2200081X.

Cybercrime and International Law, Jurisdictional Challenges and Enforcement Mechanisms. *African Journal of Biomedical Research*, 2024 (3). Available at: https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/2101?articlesBySimilarityPage=11

David S. Wall: *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, Polity Press, 2024, https://www.researchgate.net/profile/David-Wall-7/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition/links/65c36f3179007454976a5420/Cybercrime-The-Transformation-of-Crime-in-the-Information-Age-2nd-edition.pdf.

E-SPIN, AI-Powered Cybercriminals Rising, Evolution, Tactics, and Defense Strategies Against Advanced Digital Threats, Global Themes and Feature Topics, 2024. Available at: https://www.e-spincorp.com/ai-cybercriminals-evolution-tactics-defense-strategies/.

European Commission, Proposal for an Artificial Intelligence Act, 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

European Commission, Shaping Europe's Digital Future, Cybersecurity Policies, 2023. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Official Journal of the European Union, L 2024/1689, 12 July 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

Europol: Internet Organised Crime Threat Assessment (IOCTA) 2022, European Cybercrime Centre (EC3), 2022. Available at: https://www.europol.europa.eu/cybercrime

FBI and International Partners Dismantle Genesis Market, U.S. Department of Justice, 2023. Available at: https://www.justice.gov/archives/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.

Glen Dario Rodriguez – Fernando Molina-Granja: The Preservation of Digital Evidence and Its Admissibility in the Court. *International Journal of Electronic Security and Digital Forensics*, 2017 (1), 3–19. Available at: https://www.researchgate.net/publication/312665626_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court

Homeland Security, Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies, 2022. Available at: https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf.

Jan Kleijssen – Pierluigi Perri: *Cybercrime, Evidence and Territoriality: Issues and Options.* Council of Europe, 2017. https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98.

Jason Firch: *Conti Costa Rica Ransomware Attack Explained*. PurpleSec, 2024. Available at: https://purplesec.us/breach-report/conti-ransomware-attack/.

Jen Easterly: *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. CISA, 2023. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Kristin M. Finklea: *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*. Congressional Research Service, 2013. Available at: https://sgp.fas.org/crs/misc/R41927.pdf.

Law No.18/2010 of 12/05/2010 relating to electronic messages, Electronic Signatures, and Electronic Transactions, published in the Official Gazette No. 20 on 17/05/2010.

Law No. 60/2018 of 22/8/2018 on the Prevention and Punishment of Cyber Crimes. Official Gazette No. Special of 25/09/2018.

Marcus K. Rogers: Recent Advances in Digital Forensics. *Journal of Digital Investigation*, 2015 (2), 102–117.

Michael McGuire: *Into the Web of Profit. The Darknet and its Facilitating Role in Cybercrime.* University of Surrey, 2019. Available at: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf.

Mike Miller: *Social Engineering Beyond Phishing: New Tactics and How to Combat Them*. 2025. Available at: https://www.auditboard.com/blog/social-engineering-beyond-phishing-new-tactics-and-how-to-combat-them/.

Mthokozisi Hlatshwayo: *Cybersecurity in the Digital Space.* Wits Business School, 2023. Available at: https://www.researchgate.net/publication/375115830_CYBERSECURITY_IN_THE_DIGITAL_SPACE.

Olukunle Oladipupo Amoo: The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System. *World Journal of Advanced Research and Reviews*, 2024 (2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438.

Nakul R. Padalkar: *Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Financial Flows.* Graduate School of Arts and Sciences & McDonough School of Business, Georgetown University, 2024. 4–13.

Patryk Pawlak – Panagiota-Nayia Barmpaliou: Politics of Cybersecurity Capacity Building. Conundrum and Opportunity. *Journal of Cyber Policy*, 2017 (1), 123–144. https://doi.org/10.1080/23738871.2017.1294610.

Pieter Matsaung – David Tubatsi Masiloane: The Role of Cyber Intelligence in Policing Cybercrime in South Africa: Insights from Law Enforcement Officers. *South African Journal of Criminal Justice*, published online November 6, 2024. Available at: https://www.tandfonline.com/doi/full/10.1080/10246029.2024.2421225.

Roderic Broadhurst: Developments in the Global Law Enforcement of Cyber-Crime. *Policing: An International Journal*, 2006 (3), 408–433, https://doi.org/10.1108/13639510610684674.

SEC v. Ripple Labs Inc., Case No. 20-cv-10832 (S.D.N.Y. 2020). Available at: https://www.sec.gov/enforcement-litigation/whistleblower-program/notice-covered-actions/award-claim-2024-123.

Yuchong Li – Qinghui Liu: A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments. *Energy Reports*, 2021 (7), 8176–8186. Available at: https://www.sciencedirect.com/science/article/pii/S2352484721007289.

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 2013, 89. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United States v. Lichtenstein, Case No.1:22-mj-00028 (D.D.C. 2022). Available at: https://www.govinfo.gov/content/pkg/FR-2024-12-06/pdf/2024-27982.pdf.

Michael Waddington: Cybercrime Trends and Evolving Cyber Laws in 2025: A Forward-Looking Analysis. *Criminal Defense Lawyer*, 2024. Available at: https://

www.linkedin.com/pulse/cybercrime-trends-evolving-cyber-laws-2025-analysis-waddington-tb95e/.

World Economic Forum, Global Cybersecurity Outlook 2025, January 2025. Available at: https://www.reuters.com/sustainability/sustainable-finance-reporting/esg-watch-companies-complacent-about-cybercrime.