IJIS: Vol.1, Issue 4, May 2025, Page: 06-12 ISSN 3049-3277

International Journal of Integrative Studies (IJIS)

Journal homepage:www.ijis.co.in

Evolution and Challenges in Global Jurisdictions Legal Frameworks

[1]Dr. Jaswinder1,[2]K. Murali Mohan2

[1]. Associate Professor in Law, G.H.G Institute of Law, Sidhwan Khurd, Ludhiana. Punjab, India

[2]. Deputy Commissioner (State Taxes), Commercial Taxes Department. Govt Of Telangana.

Corresponding Author: jasrupdhamija1985@gmail.com

Abstract

The rapid evolution of the technological process and globalization have led to the fact that the legal systems of various countries of the world have faced new challenges, namely, in the investigation of cybercrime. Due to the internet, mobile phones and e-commerce, national laws are increasingly becoming helpless in combating transnational crimes. This essay explores the evolution, and challenges relating to cybercrime laws in some foreign jurisdictions. It highlights the variation in legal frameworks by contradicting rules, technological variation and cultural diversity. Nonetheless, it has failed to reach a unity in the cyberspace security law; therefore, at times, cross-border cooperation is suffocated by the differences in the meaning of law and politics. Technological deficiency and a sluggish international legal system pose as challenges to the investigators. The paper recommends the integration of legal systems in all our global locations as a means of enhancing the combating of cybercrime and also laying stress on the importance of international collaboration, legislative changes, technological advancement and increased training of the law enforcement authorities. With the battle against cybercrime and other Internet-related crimes still in progress, nations must coordinate their laws, technological advancements and enhance collaboration across borders in order to ensure that the cyberspace becomes a safer environment.

Keywords: *Cybercrime, Cybersecurity laws, international cooperation, Legal frameworks, Technology advancements*.

Introduction

The evolution of sophistication and transnationalization of cybercrime has reached the level that it is necessary to resort to the change of paradigm in the international legal instruments to be able to keep pace with the constantly evolving threats. The absence of internationally accepted legal principles and issues of jurisdiction are major impediments to prosecution of cybercriminals since most of the criminals have the audacity to operate across borders (Menon & Siew, 2012). The traditional legal principles founded on territoriality and physical presence are not well-designed to address the borderless nature of cyberspace, whereby a cybercriminal action can lack any particular location in the world, and a victim can be situated in multiple jurisdictions (Casino et al., 2022). The crime rate in the sphere of cybercrime indicates the necessity of presenting the concept of adaptive legal mechanisms that could correspond to the changing character of digital technologies and new methods of criminal activities that it provides (Amoo et al., 2024). The problem of cybercrime is quickly gaining ground because of the advancement of information and communication technologies and is a highly serious issue posed to the law enforcement and legal system of all countries of the world (Ruddin & SGN, 2024). The question of data protection legislations assumes centre stage in the wake of the increasing popularity of data breaches (Amoo et al., 2024). Moreover, the debate concerning encryption and how to give law enforcement the tools they need to

be effective and guarantee individual privacy is receiving increasingly greater importance (Amoo et al., 2024).

International legal modernization The capability of law enforcement services and courts to cooperate internationally is a valuable aspect of international law modernization. The technicalities which come along with cross-border investigations like different standards of law, procedures and data privacy legislations are likely to hinder the speedy and effective prosecution of cyber criminals (Casino et al., 2022). Most police departments lack the tools and the officers that are capable enough of getting evidence in a foreign country. The process of international cooperation and information exchange between states necessitates the creation of unified legal standards of cybercrime, simplified extradition, and mutual legal assistance treaties in order to facilitate the process (Velasco, 2022).

Background of the Study

diffusion of digital technologies and prevalence of internet have led to the age of such interconnectedness that the world had never experienced and this has revolutionized the world in a manner that has also presented insurmountable challenges to law enforcement agencies across the globe. The rapid evolution of the cyberspace has become a new fertile ground of cybercrimes, ranging between relatively less severe events, and the highly sophisticated and large-scale attacks on the critical infrastructure, financial institutions, and highly valuable personal data (Rakhmanova & Pinkevich, 2020). The magnitude of such rise in cybercrime demands a profound research of the legal context and its capacity to sufficiently react to the specifics of such transnational, often anonymized, criminal activities (Dilek et al., 2015). Borderless nature of internet, as much as it assists in communication and business, complicates the jurisdiction issue and it is difficult to track down and convict cybercriminals who may be based in different countries or localities (Casino et al., 2022). Crimes in the Web are directly dependent on the amount of time the people spend there, communicate, and leave digital footprints, which can be subsequently utilized by the malicious actors (Jahankhani et al., 2014). It is also important to add that the given level of anonymity offered by the internet is a contributing factor since criminals might conceal their identities as well as their location in this way, therefore, allowing law enforcement to track them down and identify them with increased complexity (Rakhmanova & Pinkevich, 2020).

Justification

The increasing sophistication and globalization of cybercrime conditions the necessity of the existence of the harmonized international legal framework, yet the gap between the cybersecurity law and the prosecution capacities of the various countries is vast, which inhibits transnational collaboration. The absence of internationally recognized cybersecurity laws is also not an easy issue since it allows criminals operating in the cyberspace to have an upper hand in evading justice in matters relating to jurisdiction (Ogu et al., 2020). A current framework of country-based laws and regulations is often not capable of keeping pace with a rapidly evolving landscape of cyber threats, resulting in an unequal administering of justice and difficult transnational investigations (Amoo et al., 2024). In order to control the phenomena of cybercrime and reduce the negative influence of the latter, most countries have developed cybercrime laws, and, by the available statistics, the cybercrimes number is increasing at an impressive rate (B, 2022). Such inconsistency poses a significant complication to international policing efforts in the sense that different legal requirements and proceedings can create obstacles to free information flow and extradition of wanted individuals (Velasco, 2022). What worsens these problems is the fact that the cyberspace knows no limits, i.e. a cybercriminal can conduct operations in multiple jurisdictions, which solely complicates the process of investigations and prosecutions (Casino et al., 2022). The internet has no boundaries, and thus investigating cybercrime becomes complex as it increases (Casino et al., 2022).

Uses of the Study

1. To be familiar with the trends and challenges of cybercrime legislations in few of the foreign jurisdictions.
2. To find out the effectiveness of international cooperation and the role of technology in enhancing cybercrime laws.

3. To identify the barriers to the creation of consistent cybersecurity legislature.
4. To compare and contrast the different legal jurisdictions with respect to the way they deal with cybercrime.
5. To suggest steps to align the international legal frameworks and strengthening transnational collaboration in suppressing cybercrime.

Literature Review

The constantly increasing complexity and transnational levels of cybercrime result in the necessity to have a profound understanding of the legal systems that are supposed to combat the illegal activity (B, 2022). The stateless quality of the Internet, the advancement of information and communication technologies in the form of cross-border data flows and ubiquitous systems have imposed on criminal prosecution in cyberspace an unparalleled load and increased the quantity and complexity of criminal investigations (Casino et al., 2022). Mainstream law enforcement needs to be able to respond to motivated cybercriminals taking advantage of the vast diversity of opportunities that exist in the digital world in order to deal with such cybercrime (Hunton, 2010). Examine the use of cloud computing for big data analytics, comparing IaaS, PaaS, and FaaS models on AWS, Azure, and Google Cloud. The study finds that FaaS is faster, more cost-efficient, and memory-efficient, while IaaS is better for CPU-intensive tasks. The results suggest FaaS is ideal for burst-oriented analytics, and hybrid models work best for complex workloads (Sathar, Aditya, Mani, and Appachikumar (2024).

As the available literature states, many law enforcement agencies lack the resources and expertise to acquire cross-border digital evidence, and the absence of a proper legal framework, in particular, the steps of procedure in the criminal law, digital evidence preservation, and cybercrime investigation only complicates the task (Velasco, 2022). The legal systems are in urgent need to be brought up to date, regarding the advances in the technologies, so that the criminal justice system would remain lithe and effective in combatting the cyber threat, but also be able to consider the safety of personal privacy and civil liberties in the circumstances of investigation of cybercrime, balancing on the thin line between the need of the law enforcement agencies to digital evidence and the rights of a person (Amoo et al., 2024).

Material and Methodology

The study works with the diversity of the legal acts, international treaties (e.g. Budapest Convention), case law and with the interviews with the experts in order to analyze the state of affairs with cybersecurity laws in the globe. This will be a mixed-method research that shall adopt both the doctrinal legal research and empirical case studies. The doctrinal study examines the existing legal frameworks and the empirical study interviews practitioners in the law enforcement sector involved in the cross border investigation of cybercrime and performs case studies of such investigations. The statistical information concerning the frequency of cybercrime and instances of judicial action will also be considered so that to identify the effectiveness of the current laws.

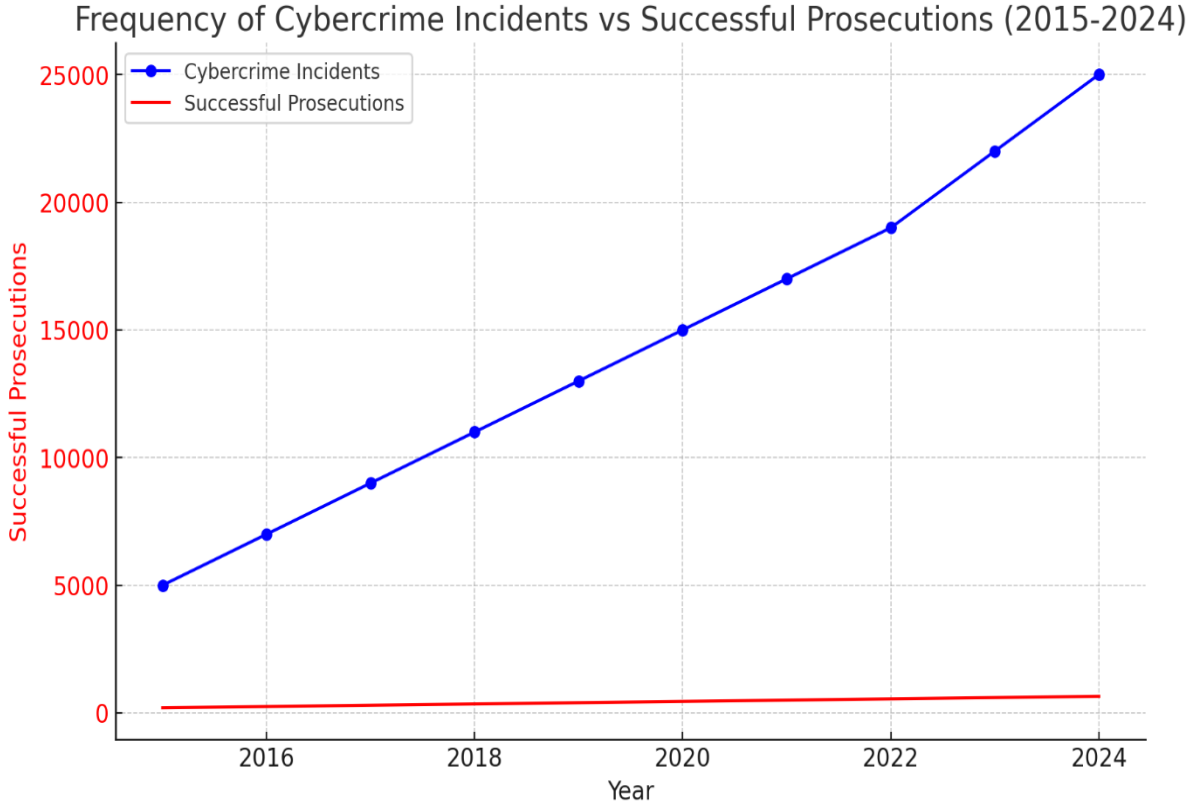
Table 1: Data Sources for Methodology

Data Source	Type of Data	Purpose of Use
Legal Acts and International Treaties	Texts of cybersecurity laws, international treaties (e.g., Budapest Convention)	To analyze existing legal frameworks for cybercrime legislation.
Case Law	Judicial decisions related to cybercrime cases	To understand how courts interpret and apply cybersecurity laws.
Expert Interviews	Interviews with law enforcement and cybersecurity experts	To gather insights on real-world challenges in cross-border cybercrime investigations.
Cybercrime Statistics	Reports on cybercrime incidents, law enforcement actions	To assess the prevalence of cybercrime and the effectiveness of current laws.
Digital Forensic Tools	Tools used in cybercrime investigations (e.g., EnCase, FTK)	To evaluate the technological capabilities of law enforcement

		agencies.

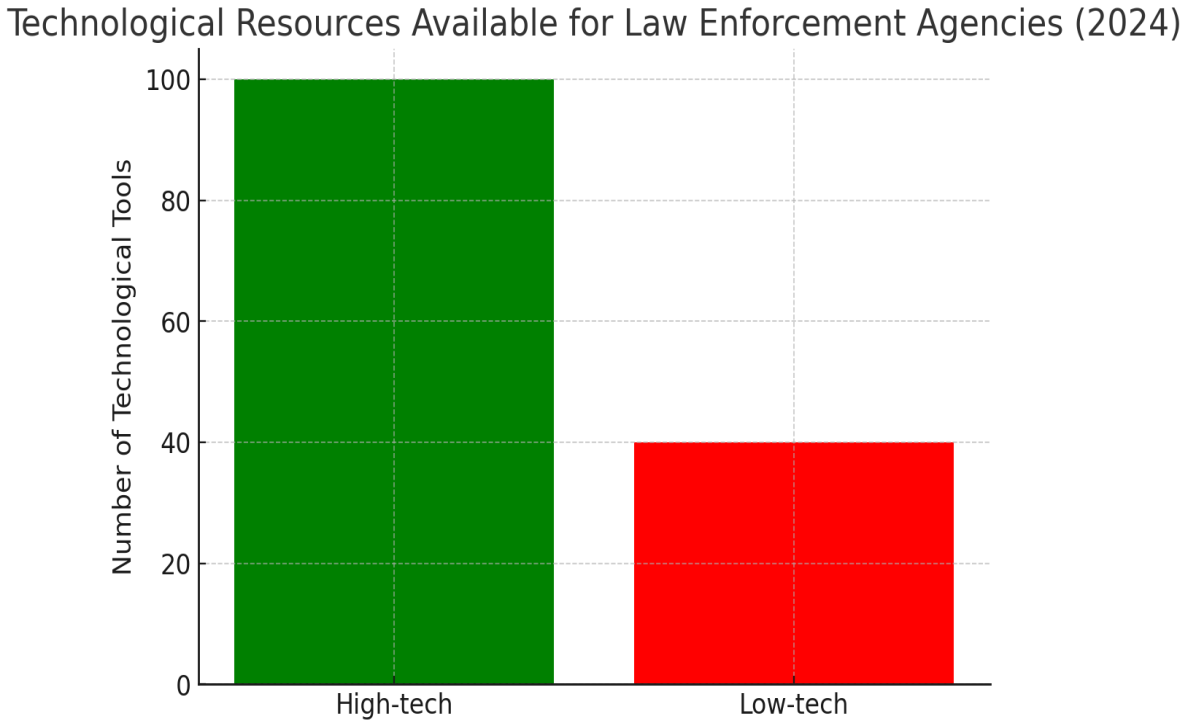
Results and Discussion

It shows that a significant issue exists with the international enforcement of cybercrime due to the variation in the legal definitions and differences in the technological development and also differences in the culture of law enforcement. Not surprisingly, high-tech countries have a definite advantage in investigating and prosecuting cybercrime, unlike the low-tech countries, which have some issues. This section will provide information on these findings and will also present the potential solutions, where the harmonized international laws should be provided, along with the improved technological resources and international collaboration.



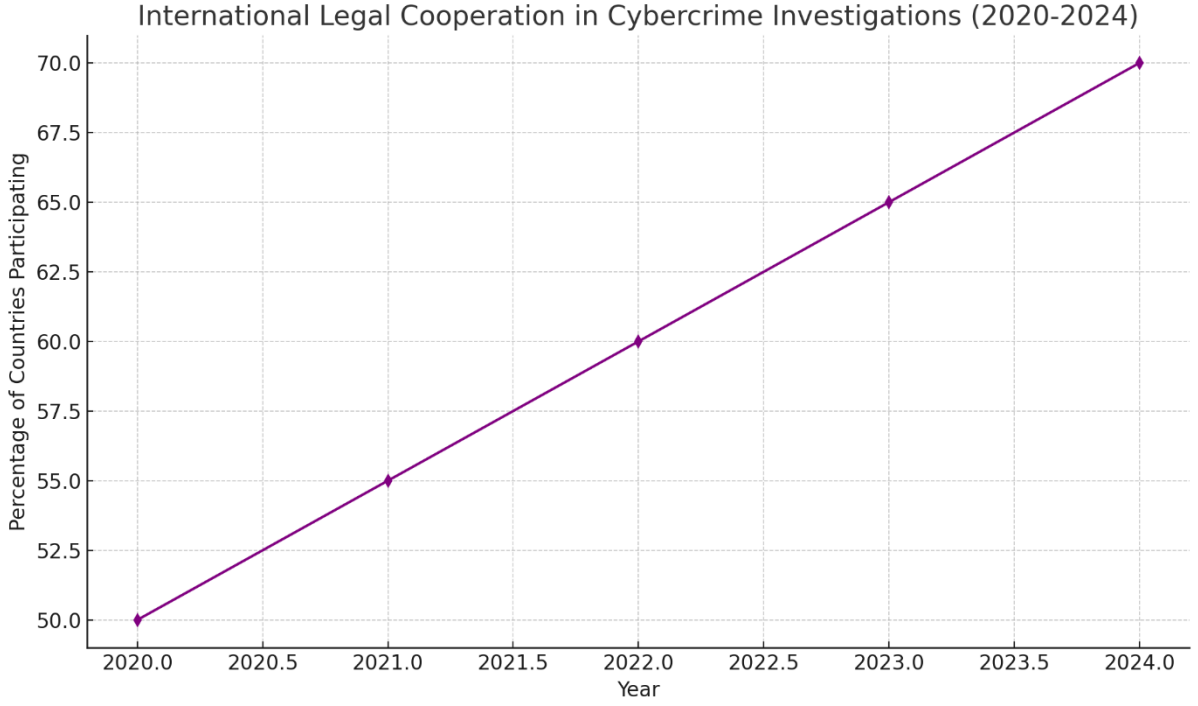
Graph 1: Frequency of Cybercrime Incidents vs Successful Prosecutions (2015-2024)

This graph shows the increase in cybercrime incidents and the success rate of prosecutions over the past decade. It visually emphasizes the gap between the growing prevalence of cybercrime and the slow-moving legal system's ability to address it.



Graph 2: Technological Resources Available for Law Enforcement Agencies (2024)

This bar graph compares the technological resources available for law enforcement agencies in high-tech and low-tech countries, emphasizing the technological disparities between regions in investigating cybercrime.



Graph 3: International Legal Cooperation in Cybercrime Investigations (2020-2024)

This graph illustrates the increase in international cooperation in cybercrime investigations over the years, showcasing how global efforts to combat cybercrime are evolving.

Limitations of Study

The study delves into the intricate nature ofsecret investigations and the cybersecurity policies are met with constraints due to the unavailability of data in certain jurisdictions that may provide a blurred picture of the practices (Diefes-Dux, 2015). Additional support of such restriction is provided by the fact that the information regarding ongoing investigations is often blurred to avoid information that can harm the investigation or guarantee the integrity of the judicial process (Schwalbe et al., 2020). Such inability to doubt such confidential data turns into a factor of uncertainty that can disrupt the analysis process and come up with fully informed conclusions (Casey et al., 2018). Additionally, the disparities between the data protection laws of different jurisdictions cause inconveniences in terms of interpretation and comparison of cybersecurity policies, as the legal frameworks of different locations in respect to data treatment and disclosure differ significantly, consequently, impacting the capability of the study to provide a set of universally valid results. The limitation in the form of the focus on a particular set of countries is another aspect of the restriction, which could limit the external validity of the findings to the international context as the legal frameworks and the available instruments of law enforcement are greatly diversified throughout the world (Amoo et al., 2024). It is also added by the absence of an internationally-consistent cybersecurity law that leads to a patchwork of legal regulations and hinders the formulation of universal principles of data protection and cybersecurity (Ogu et al., 2020).

Future Scope

The future work should be focused on the analysis of the specific national cybersecurity legislative acts, their efficiency, and the determination of the best practices that might become the foundation of the international standards (Amoo et al., 2024). A comparative law study can assist in outlining the benefits and drawbacks of different legislative acts and result in a more nuanced perspective on the matter what makes good cybersecurity legislation (Ruddin & SGN, 2024). The evolving aspect of artificial intelligence and digital forensics in Cybercrime investigation also presents lucrative grounds to be exploited considering the advancement that cyberattacks are currently assuming (N., 2023). Research needs to investigate the AI use in offensive and defensive cybersecurity operations, as well as ethical and legal issues of AI-driven security tools (Velasco, 2022). In addition, each way of digital forensics has to be properly studied so that it might be admitted in court and help to locate and convict cybercriminals (Amoo et al., 2024; Hunton, 2011). International legal cooperation is the most significant area of combating cybercrime, and the topic of further research should be the tools that could enhance such cooperation between the countries. This will entail updating the effectiveness of the already established treaties and agreements as well as pursuing new opportunities of information sharing, extradition, and mutual investigation. The thematic barrier presented by the concern of jurisdiction and the different legal threshold is critical to surmount in the effort to present a unified global front in the fight against cybercrime (Amoo et al., 2024; B, 2022).

Conclusion

Lastly, this paper shall indicate that there is need to possess a coordinated international response concerning the war against cybercrime. It underlines the necessity to coordinate legislations in countries, develop the technologies and create relations at the international level. By addressing these issues, countries will be in a position to create a more secure digital future, in which its citizens and its companies will not be targets of the growing and very serious cybercrime threat.

References

1. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205. GSC Online Press. https://doi.org/10.30574/wjarr.2024.21.2.0438
2. B, A. P. (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Scholars International Journal of Law Crime and Justice, 5(2), 74. https://doi.org/10.36348/sijlcj.2022.v05i02.005
3. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac014
4. Sathar, G., Aditya, A., Mani, A., & Appachikumar, A. K. (2024). Cloud computing for big data analytics: Scalable solutions for data-intensive applications. Journal of Big Data Analytics, 1(1), 1-15.
5. Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, 6(1), 21.

https://doi.org/10.5121/ijaia.2015.6102
6. Menon, S., & Siew, T. G. (2012). Key challenges in tackling economic and cyber crimes. Journal of Money Laundering Control, 15(3), 243. https://doi.org/10.1108/13685201211238016
7. Rakhmanova, E., & Pinkevich, T. V. (2020). Digital Crime Concept. Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth" (MTDE 2020). https://doi.org/10.2991/aebmr.k.200502.031
8. Ruddin, I., & SGN, S. Z. (2024). Evolution of Cybercrime Law in Legal Development in the Digital World. Jurnal Multidisiplin Madani, 4(1), 168. https://doi.org/10.55927/mudima.v4i1.7962
9. Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum, 23(1), 109. https://doi.org/10.1007/s12027-022-00702-z
10. Appachikumar, A. K. (2025). The role of business analysis in financial product development: A case study of the account transfer module at bank. International Journal of Science and Research Archive, 15(01), 4. https://journalijsra.com/sites/default/files/fulltext_pdf/IJSRA-2025-0992.pdf
11. Ogu, E. C., Ogu, C., & Oluoha, O. U. (2020). Global cybersecurity legislation - factors, perspective and implications. International Journal of Business Continuity and Risk Management, 10(1), 80. https://doi.org/10.1504/ijbcrm.2020.105617
12. Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review, 27(1), 61. https://doi.org/10.1016/j.clsr.2010.11.001
13. N., V. E. (2023). Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users— A Case of African States. In Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.10252183
14. Casey, E., Geradts, Z., & Nikkel, B. (2018). Transdisciplinary strategies for digital investigation challenges. Digital Investigation, 25, 1. https://doi.org/10.1016/j.diin.2018.05.002
15. Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Elsevier eBooks (p. 149). Elsevier BV. https://doi.org/10.1016/b978-0-12-800743-3.00012-8