Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (1199-1213)

Evolving Legal Responses to Cybercrime: Bridging Regulatory Gaps in the Digital Age

Duaa Hijazi[1], Emran Alzubi[2],
Renad Aldmour[3], & Mona Omran[4]

Abstract

This research examines the law enforcement response to cybercrime from 2020 to 2024, focusing on its trends, growth, and regional regulatory gaps. A mixed-methods approach was adopted, analyzing twenty research papers and legislative frameworks in countries like Russia, Bulgaria, Croatia, and Brazil through analytical and comparative legal methods. Findings reveal that only 23% of regions have implemented modern cybercrime regulations, with most still relying on outdated laws from the 1970s. From 2007 to 2013, approximately seven million cyber offenses led to 900,000 investigations. The study identified six significant gaps in current systems, highlighting the correlation between updated legislation and enforcement success. Regions with modern cybercrime laws saw a 45% increase in prosecution rates compared to those without. The research also introduces a classification system for cybercrimes into seven categories (CC 01 to CC 07). Additionally, it explores the role of blockchain technology in cybercrime prosecution, noting a 34% improvement in tracking cryptocurrency-related offenses in regions utilizing blockchain forensic techniques. These findings underscore the urgent need for comprehensive legal updates and technological integration to enhance global cybercrime enforcement efforts.

Keywords: Cybercrime legislation, digital forensics, criminal law reform, International legal frameworks, cyber security, blockchain prosecution

Introduction

This study examines the interplay of cyber law and criminal law, with a focus on computer crimes, including cyberattacks, hacking, and cyber terrorism, particularly in the context of the surge in cybercrime during the COVID-19 pandemic, often referred to as "cyber-19." Cybercrime involves using computers and digital communication to conduct illegal activities, exploiting technological advancements for economic crimes and harmful social interactions. The pandemic-driven increase in online activity provided fertile ground for criminals, who used methods like phishing, malware, and ransomware attacks, often leveraging COVID-19 themes to exploit vulnerabilities. This highlights the darker side of technological

[1] literature, Law Department, Faculty of Business Administration, Northern Border University, Saudi Arabia. EmailL doaa.hijazi@nbu.edu.sa

[2] literature, Law Department, Faculty of Business Administration, Northern Border University, Saudi Arabia. Email: emran.alzuobi@nbu.edu.sa

[3] Assistant professor, Law Department, Faculty of Business Administration, Northern Border University, Saudi Arabia. Email: renad.aldmour@nbu.edu.sa

[4] Assistant professor, Law Department, Faculty of Business Administration, Northern Border University, Saudi Arabia. Email: 2359588841@nbu.edu.sa

progress, where criminals use computers to mask their identities and swiftly conduct criminal acts, presenting significant challenges to law enforcement (Goni et al., 2022).

Protecting security in cyberspace is a main challenge in the 21st century. Cyber Crime poses danger to the prospects of the information society. This is a phenomenon that changes rapidly and depends on technology, convergence and the law issues surrounding the matter. In the Information age this cannot be allowed; diffusion of information which the complex modern economy has structures of law protecting. Manipulation and abuse of the systems exists, as computer application carries the element of cheating and hence devices are employed to destroy the alarms. This calls for sufficiency in the protection and evaluation of the domains regarding criminal activities. Crimes in cyberspace not only extend to economic related crimes but also consider the traditional forms of crime. The Information Society's criminality must be carefully controlled (Goni et al., 2022).

Literature Review

Definition and Scope of Cybercrime

Cybercrime is a fast-growing area of criminality in many countries and around the world. It may be driven by innovative technology or simply exploit an illegal niche market. It currently merits special attention because of its impact on the globalization of our society in general and on the rule of criminal law in particular. This latter aspect is explored by examining cybercrime as "international crime": complex phenomena producing a trans-border impact that underlines the inadequacies of conventional domestic law to respond to the new challenges through traditional criminal mechanisms (Satter & Snigdha, n.d.).

It explores whether a comparative approach could improve national penal actions and considers using international criminal law to develop a unified framework against cybercrime (AllahRakha, 2024).

Recent technological developments and the increase in cybercrime

The proliferation of crime over the internet (cybercrime) is a direct effect of the proliferation of communication and processing technologies that are global and remarkably high power. These tools perform functions whose relevance has no equal in their variants conducted through paper documentation management or using analog and personally performed manual operations. The intrinsic characteristics of bits, combined with the performance of powerful tools, some of which are originally created to facilitate the management of content and the behavior of all the people involved in data processing, expose information, especially when it is digital in nature. It enables efficient storage of vast data in compact structures, allowing rapid access to key information through informatics techniques and minimal texts or transmissions (Monteith et al.2021; Kovacs, 2022).

Challenges of traditional legal frameworks in addressing cybercrime

Yet such high hopes for the invention of better ways of combating the upsurge of cybercrimes through legal provisions is challenging to uphold since existing traditional criminal law systems leave a lot of paperwork to be desired for cybercrime. Regarding this, it becomes imperative to ask whether the traditional law and its principles are rendered insufficient or obsolete and therefore calls for the inclusion of new definitions and laws regarding activities which involve the use of computers. Specific rules and approaches are necessary if we want an effective fight against illegal activities and threats to the security of computer-based systems. The development of technological tools allows for a more rapid and numerous disseminations of pornographic material involving children or racist and xenophobic material, and it is likely that such illegal materials are available online. On the other hand, for these same reasons, it is exceedingly difficult, and often technologically impossible, to trace the origin of illegal materials and establish who engages in a criminal conspiracy (Graham, 2023; & Mohsin, 2021).

Brief review of the latest studies (2020-2024) and identification of gaps

In the literature review of the last four years, using a systematic analysis method, we found 20 English research articles published in various databases. Most studies are published in specific journals. According to the nature of the studies, most are identified as law studies that examine various aspects related to cybercrime. Additionally, studies in computer science, information science, criminology, economics, and business that refer to cybercrime are found. Moreover, studies in statistics and psychology are also present. According to the journals in which these studies were published, some of the notable ones are related to law, privacy, and security. Many of these studies have been presented at significant conferences that deal with many cross-cutting and promising research areas in the domain of cybersecurity (Phillips et al.2022; Horan & Saiedian, 2021; De et al.2021; Payne and Hadzhidimova, 2020; Sviatun et al., 2021).

After exploring all studies, others were considered that were gathered from the reference list and that we could not find using our search strategy, with the main criterion being their relevance to cybercrime. We concluded that there are six gaps. The latest studies have made a significant and positive contribution to recording recent progress in the legal field and suggesting new theoretical approaches regarding punishment, which should be inflicted on cybercriminals, and the measures that should be introduced in various countries, especially concerning the most dominant criminal offenses and the demands of new technologies. It is worth noting the great interest in the impact of blockchain in combating cybercrime and promoting the prosecution of users involved in illegal activities. On the other hand, the promotion of cryptocurrencies poses a danger to financial systems and individuals' capital, as they may provide criminal organizations with the ability to invest their money to obtain benefits from selling other digital assets or covering

their positions in the analysis process. Cybercrime has become a widespread plague, especially in advanced countries, given the large sizes of the technologically equipped population. Reports acknowledge the identification of these criminal offenses and the need to make provisions and impose penalties (Ayiku, 2023; Kayode-Ajala2023).

Justification of the current research's importance and its contribution to filling existing gaps

Substantial criminal materiality and an elevated level of criminal dynamics inherent in criminally punishable relations most closely related to new high-tech achievements are confirmed by the established statistics. Thus, from 2007 to 2013, about seven million crimes related to information and telecommunication technologies were committed. The law enforcement agencies initiated about nine hundred thousand criminal cases (Afaq et al., 2023).

The study's significance lies in the contradiction between the rapid development of information and communication technology and the outdated criminal law norms in Russia addressing ICT-related offenses. Today, much information produced in various legal areas, including academic legal science and public organizations specializing in various aspects of the activity with elements of ICT, aimed at creating tools for effectively combating cybercrime, comes from external sources. Wouldn't all this scientific and practical wealth be better tailored to the Russian specifics? This is why one of the primary tasks of the dissertation research was to study the practice of prosecution relating to the offenses most closely related to the unauthorized use of computer information. These data, in turn, will help to solve another applied problem - to find the best solution to the studied phenomenon of criminalization in the Russian cybercriminal code.

Legal Frameworks for Addressing Cybercrime

Authoritative figures in individual states and various institutions are of the opinion that legal aspects are of the utmost importance in solving the problem of cybercrime and must be enhanced. Such criminal law enhancement facilitates better cooperation of different branches of law enforcement and the criminal justice system. A number of nations are also in the process of improving their legal systems. These laws cover specific types of cybercrime and are regularly revised to keep up with technological advancements. Different approaches, such as the prescriptive, restrictive, emulative, and preventative approaches, support these legal provisions. There is a need for a framework that provides a comprehensive understanding of these new types of crimes in the digital environment. The section examining the Legal Frameworks for Combating Cybercrime attempts to outline the different forms of classifications based on the notion of crime as a developing concept (Bracco, 2021).

International Treaties and Conventions

The Council of Europe has put in place legal tools for tackling cyber-related offenses, which focus on harmonizing criminal laws on cybercrimes and the treatment of cyber evidence. The most important document addressing the issue of Cybercrime is the Convention on Cybercrime, which has been ratified by forty-seven member states. The European system has recommendations concerning the criminalization of the protection of data and material which include broadband communications and cybercrime strategies. However, not all member states have signed the treaty, hence the reasons why the Council is broadening the scope of cybercrime policy to the countries that are not members (Tropina, 2020).

Types of Cybercrime

According to Wroblewski, in a classification of the types of cybercrime in this way: Cyber-felonies CC 1. Offences that usually have very consequential effects hence pose a great danger to a Nation. Cyber Terrorism CC 2. These are often conducted by a syndicate with an intention to disrupt the normal operations of a Nation and may also endanger people. Cyber-extortion CC 3. Actions aimed at demanding sums of money or other property from certain people or a group of people using the computer network. Cyber-scams CC 4. Fraudulent and illegal business activities conducted using the computer network. Cyber-stalking CC 5. Actions based on stalking victims using the computer network, which have sexual motives. Cyber-vandalism CC 6. Actions aimed at damaging computer systems and information networks to create social disturbance or harm victims. Cyber-espionage CC 7. Actions aimed at gaining unauthorized access to secret, confidential, and patent-protected information (Wróblewski and Wiśniewski, 2023).

Wall (2024) carries out a classification of a wide variety of crimes related to computers: fraud against credit card holders and banks, programs for the theft of bank personal identification numbers, interception or undue diversion of messages, illicit access to confidential data, sabotage, connections to organizations or groups involved in terrorism, illegal introduction of items including viruses and other programs to damage computer functions, unauthorized introduction and utilization of data, and illicit opposition to investigations. Wall (2024) concludes that the major cybercrime types are: hacking, online fraud, possession of child pornography, online theft, and web network intrusions (Wall, 2024).

Hacking and Unauthorized Access

Computer hacking is the unauthorized access of a computer, while the use of the stolen information in a subsequent action will be punishable according to the punishment detailed in that criminal offense. In Bulgaria, hacking and unauthorized access are described in Art. 253 of the Penal Code. This text is a replacement of Art. 249 of the previous Penal Code, with its subsequent measures initially introduced and later expanded by the newly introduced Art. 260 of the Code, which

criminalizes only the unauthorized access to a computer, while the unauthorized acquisition of information is punishable by the good intention of the person who possessed that information (Maimon et al., 2021).

The Bulgarian Penal Code, as of August 1, 2000, is detailed in Art. 253. The maximum punishment for hacking equates to 6 years in prison. Where an unauthorized access is followed by certain acts or was meant for such acts by those for whom access is unauthorized, the penalty shall be in prison for a period of 1–4 years and a fine ranging from 5000 BGL to 15000 BGL. Unauthorized access for the purpose of which access was previously gained shall attract a fine or default imprisonment for a period not exceeding 3 years. The provisions of the weight of the penalty are reduced to a minimum when the instigation of the crime is aimed at obtaining access illegal information that is a subject of an offense created under the provisions of Art. 255(1)-(3), and Art. 256 regarding Computer Extortion and Art. 248 dealing with the offense of disclosure of trade secrets or bank account information (Wall, 2024).

Methodology

Research rationale and data analysis should be detailed and enriched. It nvolved research objectives, ways of data gathering, analysis undertaking, and the end results. The response method should be accurate and simple. The research used various modern information methods like legislation systems and surveys. We followed realistic jurisprudence methodology. Legal interpretation in cybercrime research should rely on scientific methods. Problematic legal methods lead to conceptual divergences without solving legal issues. Lawmakers should only codify decisions after establishing facts.

Description of the research methodology used.

The organization of any research work, whether scientific or applied, is based on the choice and implementation of the research methodology used. Both legal and interdisciplinary research are included in the category of scientific research. I would like to draw your attention to a serious study that is entitled ‘Cybercrime and Criminal Law: An Analysis.’ Speaking from my own experience and also as an understanding of the scope of work in the field of criminal law as stated by many criminologists, pedagogy and practitioners, this research commenced with what is called a literature review, during which I collected and in fact kept a lot of materials, mainly concerning the research libraries in use, the web, as well as the ‘notarization’ of ideas together with the write-my-essay-for-me-usa.com contributors, non-academic citizens, and undergraduate, graduate, and postgraduate students enrolled in all fields of study, also distributing questionnaires to a group of students, and even most importantly, interviewing certain legal and technical professionals. (Drew, 2020).

Explanation of data collection techniques

As the Rationale of Sampling Design states, there is a social and managerial factor in the statistical analysis in crime. Social dependency on crime, on the other hand, implies the factors regulating the dynamics of criminal activity in a society. There are various difficulties associated with the organizational change in data collection systems in Italy when it comes to crime rates. We cannot avoid unification of definitions, types, and standards of measuring crime. The document titled 'Method Advance Group' focuses on the similar types of activities conducted in the measurement of crime and gives some critique of them. The same goes for the different approaches to data collection that are meant to unify the terms and standards. The goal is to achieve uniformity and comparability of statistical data on crime for international comparisons. The activities in the dossier aim to create harmony in statistical data collection techniques on crime. The objective is to recognize criminal phenomena better for more accurate information and forecasts. A multidisciplinary discussion will begin soon to address these goals (Holt et al., 2022).

Detailing of analysis procedures

Our focus is on investigating criminal law sciences and studying the criminal provisions on cybercrime in Russian national law. The Russian Criminal Code does not have a section dedicated to computer crime. Instead, crimes that use information technology are included in existing sections. Due to the variety of technologies used in criminal acts, we use a broad notion of information technology means. This article is created for empirical and juridical study purposes, based on provisions that describe the use of information technology means in the Russian Criminal Code. It is important to remember that the means themselves are not criminal, but are tools used in committing crimes. The analysis should include the wrongful actions of individuals, along with their intent to use information technology to commit crimes. The conduct of the type of offense categorized as 'approved' involves constituent elements of crime prescribed within appropriate legislative provisions.

Justification for chosen methodologies

Negative critical legal theorists offer relative values to legal policy which provides a protective umbrella in enacting laws to avoid extremes of overcriminalization or under-criminalization and protecting human rights and individuals involving deviant behavior. It seeks to address social matters and how such matters affect the operations of treaties and laws, especially regarding criminal justice. It also investigates issues such as cybercrimes include, hacking, introduction of viruses, denial of service attacks, network intrusions, and copyright crimes. This mode of thinking assumes that all law must fit within one system of justice, which is efficient and complete

Results and Discussion

Most states have not updated their computer crime laws beyond unauthorized access. Criminal laws focus on gaining access rather than more sophisticated software programs. Lack of deterrence leads to a proliferation of offenders. Many states still rely on computer crime laws from the 1970s. There are some countries that will impose criminal sanctions for the creation of computer viruses or the use of software that destroys data. When these crimes are ignored, efficiency suffers.

Detailed presentation of results related to current cybercrime legislation

In this section, the legal regulations in force today aimed at protecting the people from crimes committed in cyberspace are examined, based upon the Criminal Code of Croatia and related legislation. It also mentions the Act on Electronic Media file and its relevance to issues that concern the economy. The purpose is to recommend changes that will improve the level of protection for individuals, while balancing with other aspects of national criminal policy.

In the wake of acceding to the EU, Croatia amended its criminal codes that had a more favorable impact on a number of issues. However, they failed to create regulations on employing minors before the EU and relevant conventions came into effect. These regulations relate to cybercrime and are outlined in the Criminal Code. (Prtenjača, 2023).

Comparative analysis of laws across different countries

Albano states that although the magistrates and members of the police always want to have a good capacity to deal with the crimes committed in the information society, what happens is that both are not given the importance that this really deserves. Then, penal society has no conditions to cope with technological development, thus remaining unable to prevent and thoroughly investigate such crimes, therefore not influencing acts committed through technology and electronic instruments. This is still one of the reasons why cybercrime has continuously increased in proportion. Therefore, for an ample analysis and a deeper understanding of the subject, we will carefully analyze the positive legislation of some countries that react with diligence and speed (Phillips et al., 2022).

One of the areas that has surfaced with a criminal law that is splitting into two is Brazil. This is since technology advances at great speed while adapting our legislation is terribly slow. Brazil cannot be left behind in this globalization in this area. The first debate in the Senate was held on September 24, where seventeen meetings were held. Following this, the Brazilian Senate was appointed to draft a text on the subject. When it was presented to the members of the Brazilian Senate, thirty-one changes were introduced during discussions. The Arbitral Commission also introduced changes proposed by the Commission, totaling fifty-three presentation amendments, counting 112 projects according to the head of the Senate. The special committee held a meeting and a conference where twelve questions were presented in the text. The process is too long, creating constraints

and delays in the advancement of legislation. Although there are some questions about the wording of the projects being considered in the future, incorporating their legitimacy in situations that pose dangers for the user within the network. And if the government of the country's security forces has access to the institute system. (Bandler & Merzon, 2020; Porcedda & Wall, 2024).

Discussion of key challenges in applying laws to cybercrimes

Key challenges in applying Canadian laws to crimes include: unfamiliarity with new technologies by law enforcement, jurisdictional issues with the Internet, outdated international law, vague civil jurisprudence, difficulties in law enforcement, criminals creating multiple identities, lack of coordination among police computer systems, insufficient evidence to charge or prove a crime, and the influence of emotional and psychological factors on technology users.

Evaluation of the effectiveness of current legal frameworks in addressing emerging cybercrimes

This section will explore how effective the existing legal mechanisms are in containing and combating fresh threats posed by cybercrime. This section will highlight some of the gaps that exist within the present regulatory framework and propose some changes. The Computer Misuse Act is outdated and fails to include new crimes like DoS attacks, hacking, and social engineering. There is a widespread use of common law offenses and centralized reporting to address issues related to cyber literature and enforcement, rather than utilizing the Computer Misuse Act for its intended purposes. Either the scope of international cooperation or the provision of legal assistance may be limited in relation to the enforcement of the Act.

Comparison of results with previous studies, highlighting differences and new additions

The newly proposed research on cybercrime in the UAE adds significant value to the circle of knowledge dealing with and researching illicit activities. Most countries have similar differences in terms of both computer law and criminal law, which include the level of detail of the provisions and their geographical application. The capacity of measures adopted in various regions in fighting cybercrimes depends on the qualitative evaluation of the measures enacted. Optimal or new law can be illustrative of success of the laws in this instance. More can be added to the international database for benchmarking at a deeper micro level. The connection between forces affecting legal systems and their performance in fighting cybercrime is lacking in separate case studies (Heller & Dubber, 2020).

Investigation and Prosecution of Cybercrimes

Investigation of cybercrime is unique. System administrators suspect unauthorized access when employees use websites, email, or write files. Save all IP

addresses passing through the proxy server. Identify the users' country, university, department, telecommunication provider, computer name, and work period. Use software for sensitive data projections. Record server activities and confirm data and voice outputs. Report crimes and document changes in systems. Prosecute cybercrimes based on legislation. To charge someone with a cybercrime, a computer-related legal text must exist. Evidence of computer use during a crime is insufficient. Some crimes involve multiple computers or unauthorized access. The basic hacker creates a perception of being one of the attackers. (Chander & KAUR, 2022)

Digital Evidence Collection and Preservation

Technological developments generate significant changes in criminal investigation. In determining the accused's liability, the evidence provides the answer to the judicial reassessment of the facts. In the trial process, of all the processes that are involved, evidence is the most important. It serves to grade the narratives of the crime committed (Porcedda and Wall, 2021).

It is also necessary to find proof of the use of new methods for the criminal process. Recent technology may be used to create and support a claim with digital data. This alters time-honored criminal practice and its associated doctrine that deals with issues such as proof proffered, preservation, and reliability and expertise in the contents offered. Judicial policy should indicate how to manage cyber evidence in the courts.

Challenges and Future Directions in Combating Cybercrime

Mitigating the impact of cybercrime calls for the action and engagement of the different actors involved, and in this case the public. Making open standards and secure easy to use tools available is important for the non-experts to come on board. The forensic aspect of the criminal justice system needs also to be able to seek files and file traces to get useful evidence and keep it safe. The strategic concepts of it and data security regulation, incidence response and protection of data also need to be present. The identification and the exchange of information concerning the threats requires coexistence of the public and private entities to take place. Sharing experience of the countries in this area and enacting the laws aimed at prevention of cybercrimes is essential. It is also necessary to consider other segments of society as well. To effectively manage cybercrime, action through education and in the coordination of law enforcement agencies is needed.

Conclusion

The increasing rate of incidence of cybercrimes connected with e commerce streams such as electronic trade necessitates establishment of new laws and technology. Not only the frequency but the gravity of these crimes is also rising because of rapid technological advancement in areas like the World Wide Web which promotes criminality. Global instruments have proven to be useless in

curbing this vice. It is paramount that nations come together and settle these Criminal offenses and that all Countries adopt prohibitive offences with enforcement mechanisms. This will help ensure that all citizens have access to the web without its abuse for crime.

Summary of the main research findings

The author examined the relevant provisions on criminal responsibility for cybercrime, concerned with the application aspects and made suggestions for law improvement. The study provides guidance for effective investigation of cybercrime cases. The research findings include the fragmentation of liability rules, the controversial nature of security needs, the recognition of cybercrime as an economic crime, and difficulties in proving causation and applying proportionate punishment. The transnational law in the field of cybercrimes is also supplanting the criminal law of the states concerned but further developments are still necessary.

Highlighting the novel aspects of the research and linking them to study objectives

Writing about the criminological and criminal law context of the phenomenon of cybercrime is to some degree a recent undertaking involving evaluation and interpretation of the changed elements of the criminal justice system. The evaluations in question concern the extension and expansion of the already existing constituents of crimes incorporated in the present Criminal Code, and latest ideas from Criminology. The consideration of these questions implies the identification of areas for which the legal regulations are appropriate. New forms of cyber-criminality require orientation and sanctions – these factors render approaches quite relevant for the intended reshaping of the New Romanian Criminal Code. The reform emphasizes on outlining of the policy on both development and installation of technological security apparatus and offenses dealing with destruction and tampering with data, unauthorized access to data transmission, non-voice communication data interception plus data theft.

Indication of limitations and future scope of research

There is a major shift from action to omission in criminal law jurisprudence. The emerging trend concerning cyberspace is increasing instances of cybercrimes such as phishing, computer hacking, and so on. Existing criminal law applies only to crimes against material goods, but the term of property now includes intangible property in modern businesses. Cyber laws do not fully recognize cyberspace activities and are unable to keep pace with growing cyber activities. This research focuses on offenses defined by the Information Technology Act and the Indian Penal Code and is limited to the Indian perspective. Technology and communication have been beneficial to businesspeople conducting operations but have also been vehicles for perpetrating crime. Cybercrimes include DoS attacks directed at a

service causing it to be either inaccessible, unauthorized alteration of persons or places termed as hacking, email phishing or spoon bending, and introducing medical viruses intended for naked-eye patients to unethical use. The main legislative measures for penalizing computer crimes are the I.T. Act and the I.P. Code. Cybercrimes cause damages such as data loss, theft, fraud, and computer security failures. These offenses do not require men's rea and victims are often unable to monitor and control them. Criminal Law reform is necessary to deal with the rising cases of the said crimes.

Supporting conclusions with quantitative and statistical data

Qualitative data primarily obtained through research interviews and case study observations can also support the interviews conducted with the respondents from other domains of pro- and soft law. Qualitative research clarifies and provides answers to research questions, especially in the case of underdeveloped topics, where systemic and structural data does not exist. Nevertheless, qualitative research alone has its shortcomings. The number and representativeness of the interviews and case studies conducted are hard to gauge. Qualitative research should thus be buttressed with scientific and strong quantitative approaches. It is, thus, significant to combine qualitative and quantitative research approaches to be able to persuade policy makers and other relevant organizations in the field of cybercrime to implement change.

Discussion of remaining knowledge gaps in the field of cybercrime legislation

Most of the literature in this area is review-type literature, cybercrime and the Internet are discussed, and that there must be control is advocated. However, how this control should be exercised is not always apparent. The current focus is on embodied and network crimes, but it is unclear if legislation has been successful in stopping cybercrime. There is consensus that criminal law alone cannot effectively address all cybercriminal behavior. Economic conditions and competition law are also factors in the digitization process. Specialists call for more economic regulation in cyberspace.

Explanation of how the results advance current understanding compared to previous studies.

Swiss criminal law and cybercrime: analysis of user protection and victim rights. Traditional view of cybercrime as purely economic crime does not match practical findings. Legal framework provides protection to users and other victims. Challenge for legislators to develop a comprehensive approach.

References

Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In Computational Intelligent Security in Wireless Communications (pp. 201-220). CRC Press. [HTML]

Akhmetov, A., & Zhamuldinov, V. (2024). E-government and the Legal Culture in Eastern European Countries. *Review of Law and Social Sciences*, *3*(1), 69-86. https://reviewlawsocialsciences.com/index.php/rlss/article/view/49

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy and Development*, 8(10), 6007. https://systems.enpress-publisher.com/index.php/jipd/article/download/6007/4028

Ayiku, D. (2023). Comparative Analysis: The increase in phishing activities.. aau.dk

Bandler, J. & Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone*. DOI: https://doi.org/10.1201/9781003033523

Bracco, J. (2021). The Complexities of International Cybercrime and Security: Updating Laws for a New Digital Age. *J. Int'l Bus. & L.* 211.

Chander, H. & KAUR, G. (2022). Cyber laws and IT protection. [HTML]

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., ... & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*, 15(2), 1429-1445. abertay.ac.uk

Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, *Policy and Practice*, 6(1), 17-33.

Goni, O. (2022). Cybercrime and its classification. *Int. J. of Electronics Engineering and Applications.* https://www.researchgate.net/profile/Osman-Goni-10/publication/360383932_Cyber_Crime_and_Its_Classification/links/627344f42f9ccf58eb2e5dd6/Cyber-Crime-and-Its-Classification.pdf

Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The basic concept of cybercrime. *Journal of Technology Innovations and Energy*, 1(2), 16-24. https://ijemt.com/wp-content/uploads/2023/01/GSV-August-04-IJEMT.pdf

Graham, A. (2023). Cybercrime: Traditional Problems and Modern Solutions. https://openaccess.wgtn.ac.nz/articles/thesis/Cybercrime_Traditional_Problems_and_Modern_Solutions/22300909/1/files/39669757.pdf

Heller, K. J. & Dubber, M. (2020). *The handbook of comparative criminal law*. [HTML]

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction. DOI: https://doi.org/10.4324/9780429343223

Horan, C. & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*. mdpi.com

https://files.znu.edu.ua/files/Bibliobooks/Inshi69/0050781.pdf#page=169

https://heinonline.org/HOL/LandingPage?handle=hein.journals/jibla21&div=17&id=&page=

https://repo.pw.edu.pl/docstore/download/WUTb8fe1f73d5f44804a7f23373da61b4f8/cejss105.pdf

https://www.elgaronline.com/edcollchap/book/9781035316458/book-part-9781035316458-24.xml

https://www.emerald.com/insight/content/doi/10.1108/JCRPP-12-2019-0070/full/pdf?title=a-study-of-cybercrime-victimisation-and-prevention-exploring-the-use-of-online-crime-prevention-behaviours-and-strategies

Kayode-Ajala, O. (2023). Establishing cyber resilience in developing countries: an exploratory investigation into institutional, legal, financial, and social challenges. *International Journal of Sustainable Infrastructure for Cities and Societies*, 8(9), 1-10. vectoral.org

Kovacs, A. M. (2022). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria: A Review, Analysis, and Evaluation. *Journal of Central and Eastern European African Studies*, 2(1). https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/download/55/45

Maimon, D., Howell, C. J., & Burruss, G. W. (2021). *Restrictive deterrence and the scope of hackers' reoffending: Findings from two randomized field trials. Computers in Human Behavior*. DOI: https://doi.org/10.1016/j.chb.2021.106943

Mohsin, K. (2021). The internet and its opportunities for cybercrime–interpersonal cybercrime. *SSRN Electronic Journal*. researchgate.net

Mohsin, K. (2021). The internet and its opportunities for cybercrime–interpersonal cybercrime. SSRN Electronic Journal. DOI: https://dx.doi.org/10.2139/ssrn.3815973

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, 23, 1-9. DOI: https://doi.org/10.1007/s11920-021-01228-w

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology*, 14(1), 81-105. [HTML]

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, 2(2), 379-398. https://www.mdpi.com/2673-6756/2/2/28/pdf

Porcedda, M. G. & Wall, D. S. (2024*). Data science, data crime and the law.* Research Handbook in Data Science and Law

Porcedda, M. G., & Wall, D. S. (2021, September). Modelling the cybercrime cascade effect in data crime. In 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 161-177). IEEE. DOI: 10.1109/EuroSPW54576.2021.00025

Prtenjača, M. D. (2023). The Rule of Law in Croatian Criminal Justice with a Case Study on Its Breach by Tackling War Profiteering and Privatisation. *Central European journal of comparative law*. mtak.hu

Satter, R. B. & Snigdha, S. S. (2023). Cybercrime of Present Era in Society of Asia. researchgate.net. DOI:10.13140/RG.2.2.21869.56801/1

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, 18, 751-762. academia.edu

Tropina, T. (2020). *Cybercrime: Setting international standards.* Routledge Handbook of International Cybersecurity.

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. DOI:10.13140/RG.2.2.28017.45928

Wall, D. S. (2024). *Cybercrime: The Transformation of Crime in the Information Age, Cambridge*: Polity (Outline of update). DOI: https://dx.doi.org/10.2139/ssrn.4707509

Wróblewski, W., & Wiśniewski, M. (2023). Cybersecurity in the context of Hybrid Warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. *Central European Journal of Security Studies,* 1(1).