Journal of Social & Organizational Matters
Vol 4 No 4 (2025): 255-269

Cybercrime and Digital Offenses: Challenges of Applying Traditional Criminal Law

Muhammad Ahsan Iqbal Hashmi[1], Uzair Junaid*[2], Ghulam Muhammad Mujtaba Qadir[3]
[1]Assistant Professor of Law, Department of Law, Bahauddin Zakariya University Multan (Vehari Campus), Punjab, Pakistan.
[2]Lecturer, Law University Gillani Law College, Bahauddin Zakariya University, Multan, Punjab, Pakistan.
[3]LL.M (Commercial Law), University of West of England (UWE), Bristol, UK, Advocate High Court, Pakistan.
Corresponding author: uzairjunaid@bzu.edu.pk

Keywords: *Cybercrime; Digital Offenses; Traditional Criminal Law; Jurisdiction; Actus Reus; Mens Rea; Budapest Convention; Digital Evidence; Cyber Forensics*
DOI No: https://doi.org/10.56976/jsom.v4i4.343

The spread of digital technologies has changed the character of criminal activity allowing committing crimes that do not respect the territorial borders, using anonymity and at an unprecedented speed. The traditional crime law, which is built on geographic scope of behavior and identifying criminals, has a hard time adapting to these new technologies. The continuing nature of cybercrimes like unauthorized access, data breach and cyberstalking, online fraud, identity theft and the spread of malicious code have continually challenged the basic legal principles actus reus, mens rea, causation and jurisdiction. In spite of the national legislative changes and the development of soft-law systems, inconsistency in the substantive definitions, the level of evidentiary standards, investigative authority and international cooperation remain. The paper critically examines the structural constraints of the traditional criminal law in addressing digital crimes and provides a comparative overview of the response of law in the modern times and assesses the harmonization initiatives made using mechanisms such as the Budapest Convention and regional cybersecurity standards. It claims that the key to effective enforcement, however, lies in a mixed legal approach that would provide technological neutrality and digital specific norms that would guarantee not only due process but also operational efficiency in the dynamic cyber ethos.

1. Introduction

Digital technologies have undergone swift growth in the past thirty years and radically shifted the criminal landscape of the sphere. Crimes that could previously be carried out only by being in the same place and meeting the face-to-face criteria, along with some means of physical committance, can now be performed using decentralized networks, encrypted platforms and anonymizing tools. Because of the growing adoption of digital systems in society in the areas of commerce, communication, governance and personal life, potentials of abuse have equally increased. Cybercrime, variously defined as violations of access control and financial frauds, identity theft, cyberstalking and use of malicious software have therefore become one of the most urgent issues that legal systems of the modern world face. The conventional type of criminal law based on suppositions of territoriality, corporeal behavior and linear causality cannot be useful in dealing with the fluidity and borderless character of online crimes (Holt, 2019).

One of the main challenges is the conceptual design of traditional doctrines of criminal law. Legal traditions generally support a system of well-established definitions of actus reus, mens rea and causation based on an age when harm was mostly physical and direct. Digital behavior, though, often entails intangible harm, automated systems and distributed cyber systems and it is hard to assign any liability to one actor or jurisdiction (Brenner, 2006; Graham & Smith, 2024). Besides, the transnational nature of cybercrime has complicated the implementation of traditional territorial jurisdiction, where a single online operation can see three or more servers, victims and offenders in three or more nations at the same time. This plurality creates conflicting laws, parallel prosecutions and hindrance to enforcement.

To worsen these conceptual issues are practical constraints. Investigators need to work through encrypted platforms, temporary digital tracks and platforms that cross national borders. Courts, in its turn, will have to determine how digital evidence which is fragile by its nature and prone to changes may be admissible and reliable (Stoykova, 2024). This has led to a huge disparity within the ability of legal institutions and the ability of cyber offenders to execute their activities in most states.

To counter this, national governments and inter-governmental organizations have pursued different approaches - including technology-neutral criminal law legislation and full cybercrime legislation and multilateral cooperation initiatives. Nevertheless, the inconsistencies in the legal definitions, the standard of evidence and the instruments of the process still obstruct the global attempts at harmonized enforcement (Metaxakis, 2023). These differences indicate that it is the time to have a more logical system of the law that can balance the principles of the traditional criminal law with the requirements of the digitalized society.

These challenges are analyzed in this paper in a comparative and analytical manner. It assesses the shortcomings of the law of traditional criminality in addressing cybercrimes, examines the new regulatory courses and reflects the opportunities of harmonization of approaches to cybercrimes by regional and international efforts. Conclusively, it contends that traditional legal

principles are still applicable but they need a lot of revision to respond to the unique nature of cybercrime.

2. Conceptual Foundations of Cybercrime

The conceptual fluidity of cybercrime needs to be appreciated to understand it. In comparison to the traditional crimes, whose foundations are anchored in the physical actions and the apparent damage, cybercrimes occur in a digital world that is ever-changing. Consequently, definitions are considerably divergent within jurisdictions, academic literature and international organizations. Other legal systems have taken a more limited approach where the primary aim is the offence against computer systems, including unauthorized access, disrupting of information and the propagation of malicious software. There is a wider definition used by others to include any crime assisted by or perpetrated using digital technologies such as cyber-enabled fraud, identity theft, cyberstalking and digital content crimes (Smith et al., 2023a). Lack of a unified definition makes the coherence of laws more difficult and makes international collaboration more problematic.

Cybercrime is usually divided into three main categories: (i) computer-integrity crimes, in which conventional crimes obtain greater breadth and profundity using digital instruments; (ii) content-related crimes, such as hate speech on the internet or sharing outlawed content (Wu et al., 2023). Such classifications, as useful as they are, are not flawless since new types of crimes are being introduced just to violate the traditional boundaries and are cryptocurrency-related fraud, ransomware attacks and artificial intelligence-based intrusions.

Cybercrime is also unique in terms of technological peculiarities, which make it unlike traditional criminality. Today, offenders usually abuse digital anonymity and encryption, spoofing and decentralized networks, to conceal their identity and whereabouts. The pace and automacy of cyberattacks allow causing significant damages in the course of several seconds, even without the human interference (Graham & Smith, 2024). This disconnection of action and harm is a challenge to the conventional criminal theories in which causes and effects are linear and the agency of the human is grasped.

The other underlying problem is the concept of technological neutrality in criminal law- the perception that laws would be treated equally in spite of the means involved. Technological neutrality is an attractive concept but it is hard to keep in reality. A lot of cyber-crimes reflect behaviors or damages that cannot be physically replicated and the sake of which demands the enactment of technology-sensitive laws by legislators (Heyndels, 2023). Very broad or very narrow laws are either likely to criminalize any legitimate digital conduct or to avoid addressing major conduct.

Borders and nationality Cybercrime is also transnational and borderless as compared to traditional crime. The digital activities regularly cross jurisdictions in many cases without the intention of the perpetrator. This brings fundamental issues on sovereignty, applicable law and boundaries of national criminal justice systems. With the digital space crossing the geographic

boundaries, the conventional legal presumption of locality, presence and harm by territory is becoming more tented (Hussain et al., 2023). As a result, cybercrime takes a special conceptualization that requires a re-examination of the criminal law doctrines.

2.1 Substantive Criminal Law Challenges

The conventional criminal law is rooted in the assumptions of the doctrine that assumes physical behavior, direct injury, the actors and events that are territorial based. All these fundamental aspects are disturbed by cybercrime and significant gaps emerge in the substantive principles of criminal liability. The former issue relates to the conceptualization of actus reus. Under the traditional criminal law, the criminal act is usually observable and tangible. Comparatively, abstract activities, such as unauthorized access, data manipulation or using code, are habitual to cyber-crimes and they can be carried out remotely and without leaving tangible physical evidence (Smith et al., 2023b). The question of whether a simple breach of a system is a sufficient actus reus or whether a provable injury to the integrity of data or the functionality of the system, is necessary is a controversial issue of comparative jurisprudence. Digital harm (as opposed to physical harm) is often reversible, unseen or immeasurable and this makes it hard to define the guilty behavior.

The second challenge is the determination of mens rea. Numerous cyber-crimes demand extremely precise mental conditions, but cyber processes can be robotized, contracted to bots or supported by malware that has self-propagational features. It is especially difficult to assign the intention or knowledge when the offenders make use of the anonymizing tools or take advantage of vulnerabilities without being entirely aware of the outcomes of their actions(Xiao, 2023). Moreover, some cybercrimes, such as distributed denial-of-service (DDoS) attacks or ransomware efforts, can feature various actors playing a role in a bigger operation and making complex issues of collective responsibility and the scope of established theories, such as conspiracy or joint enterprise.

Conventional criminal law is also ineffective in seeking to apply pre-digital maxims to new patterns of injury. Crimes like stealing, fraud or trespass presuppose the presence of tangible goods or fraud directed to an individual. Digital analogies, however, incorporate the unauthorized scavenging of information, the abuse of algorithms or the adoption of phishing proposals, which depend on the vulnerabilities of systems and not on inter-personal fraud (Farber, 2025). Courts in a number of jurisdictions have differed about whether information is property, whether intrusion into a digital system can be compared to trespass or whether foreign access inevitably implies a lack of honesty. Lack of clarity in the doctrines leads to inconsistent verdict and prosecution complications.

The increasing shift toward legislation unique to digital technologies has been accompanied by a discussion about whether a criminal law takes technologically neutral or technologically specific ways. Neutrality guarantees flexibility of the legal rules to technological change, but can make them overly abstract to deal with complex digital operations. On the other hand, technology-specific laws are at risk of becoming obsolete in a short period (A. Graham,

2023). Finding a compromise between these rival paradigms is one of the key issues of lawmakers trying to bring the substantive criminal law up to date.

Lastly, the spread of new forms of digital crimes, including AI-related cyberattacks, deepfake frauds and cryptojacking, proves that it is not possible to rely on ready-made doctrines alone. Unless the law is regularly adjusted, there will always be loopholes that can be used by offenders to take advantage of the mismatch between the traditional understandings of the law and the actual circumstances of the digital landscape (Wall, 2024a). Resistance to change and continuity of the doctrines are therefore the thorn in the flesh of substantive criminal law in its endeavor to deal with cybercrime.

2.2 Jurisdictional and Territoriality Challenges

The phenomenon of cybercrime being borderless is among its key characteristics and a fact that essentially negates the concept of territoriality in the world of criminal law. The majority of legal frameworks believe that criminal activity takes place within a certain geographical area and that the location of the crime is the jurisdiction of a state. On the other hand, cyber crimes regularly entail perpetrators, victims, servers and intermediaries in various countries leaving them with overlapping jurisdiction claims or, on the contrary, jurisdiction gaps (Gompert & Libicki, 2023). This spreading of behavior to various territories has created a complicated environment where states find it hard to impose themselves or what law system to apply on a crime.

One of the fundamental issues is caused by extraterritorial jurisdiction. Although most states have extended their jurisdiction in criminal acts by claiming jurisdiction over foreign-based cybercrimes, especially when national security, infrastructure and citizens are involved, these claims are usually in conflict with the sovereignty of other states. The uncertainty created by the absence of clear international norms that regulate extraterritoriality causes friction in diplomatic relationships as well as challenges in prosecuting transnational criminals (Shurson, 2023). To make things worse, cybercriminals often use what is known as safe haven or jurisdictions that lack effective cybercrime laws, have a strategic non-cooperation policy or little ability to investigate.

Such an issue as attribution makes the issue of jurisdiction even harder. Determining the geographic position of a criminal or even whether an assault was initiated by a certain nation, is notoriously challenging since there are anonymizing services, including VPNs, Tor networks, proxy servers and botnets (Irshad & Siddiqui, 2023). Attributing cyberattacks improperly would lead to improper prosecution or misplaced diplomatic reactions, which is why it is necessary to clarify the standards of evidence and international reaction mechanisms.

The other jurisdictional obstacle is the use of the Mutual Legal Assistance Treaties (MLATs) to investigate across the borders. MLAT processes, which are intended to be used in conventional criminal investigations, are cumbersome, bureaucratic and may not always suit a high-crime rate of cybercrime. This demands months or even years to gain access to data held by foreigners, digital logs or server records, which is extremely important in criminal investigations since the digital information is volatile and thus it can be lost (Zhang & Gong, 2024). This results

in systematic delays which reduce both prosecutor opportunities and deterrence to investigators. As a reaction to such difficulties, both regional and international structures have tried to formulate common jurisdiction principles.

The best tool that has been of great influence is the Budapest Convention on Cybercrime that provides an insight into jurisdiction, the powers of investigation and the liaison of nations. Nevertheless, it is restricted due to the non-participation of major cyber powers, including Russia and China, which, on the contrary, advance the models of cyber governance that focus on sovereignty (Péter, 2023). The other regional initiatives, including cybersecurity guidelines of the European Union, cyber norms of the ASEAN and frameworks of the African Union, offer valuable models, yet they are too little to offer a global regime. Such disparity of approaches highlights the continued collapse of international cyber policing and the continuous problem of aligning territoriality with the virtual nature of transnational cybercrime.

2.3 Evidentiary and Procedural Challenges

Cybercrime is a special area of evidentiary and procedural challenges on investigations that put strain on the capacity of traditional criminal justice systems. Digital evidence, whether that is emails, server logs, metadata, cloud storage logs, even cryptocurrencies is weak, volatile and can be easily manipulated. Digital data can be overwritten, corrupted or encrypted automatically, than the physical evidence, which can be stored and analyzed later, which makes it exceptionally challenging to collect and save (Kaur & Dhawan, 2024a). The integrity, authenticity and admissibility of such evidence require strong protocols to be established by the courts and investigators, but most jurisdictions have no thorough standards or technical ability.

Chain of custody is an important procedural issue of a cyber-crime case. To avoid claims of manipulation, it is important that whoever accessed, copied or transferred digital data should be properly documented. Since digital evidence is remote and dispersed, the chain of custody is difficult to verify, especially when the information is stored in more than one server, cloud computing or border jurisdiction (Shami et al., 2025). The inability to have clear provenance may lead to the rejection of essential evidence that may be used to sabotage prosecution and the belief of the population in the judicial system.

Online investigations also have an overlap with privacy and accessibility of the law. All these encryption technologies, anonymization applications and private communications platforms present obstacles to the law enforcement willing to intercept or analyze the information. Conventional criminal processes frequently fail to balance the roles of investigation with the constitutional or human rights safeguard, including the right to privacy, the protection of data and the due process (Solove, 2025). Online investigations also have an overlap with privacy and accessibility of the law. All these encryption technologies, anonymization applications and private communications platforms present obstacles to the law enforcement willing to intercept or analyze the information. Conventional criminal processes frequently fail to balance the roles of investigation with the constitutional or human rights safeguard, including the right to privacy, the protection of data and the due process.

Cyber forensics has been critical in dealing with these problems. While such forensic experts have to find a way to retrieve and investigate data, they also need to present extremely technical results to judges, juries and lawyers in a manner they can understand. Cyber forensics is an interdisciplinary field, which includes computer science, information security and legal reasoning and creates technical/procedural challenges (KAUR & DHAWAN, 2024b). The courts can find it difficult to assess the accuracy of expert testimony or adequacy of forensic procedures which increases the chances of evidentiary challenges.

Lastly, procedural frameworks need to take into consideration the global nature of digital crimes. Finally, the procedural frameworks must consider the international character of digital crimes. The search of digital evidence can also be done in partnership with foreign nations and in this case, there can be the application of Mutual Legal Assistance Treaties (MLATs) or ad hoc. The slow and bureaucratic character of such procedures can postpone the process, jeopardize the accuracy of the data or force investigators to wait until voluntary self-disclosure by non-governmental participants (Salimi, 2024). All these procedural challenges paint the picture of the pressing need of a harmonized set of standards, upgraded investigative authority and specialized prosecution education to make sure that the cases of cybercrimes can be tried effectively and impartially.

3. Enforcement and Investigative Challenges

The application of the cybercrime laws and effective investigation are complicated matters with various faces which are rooted in the technical organizational and legal complications of the digital crimes. Conventional policing organizations tend to be poorly adapted to tackle offenses that need specialized technical expertise, the capacity to act on a timely basis and co-ordination actions across state lines (Wall, 2024b). Inadequate technical skills, lack of cyber forensics training and obsolete investigation guidelines often interfere with quick detection, gathering of evidence and prosecution.

A shortage of technical competences and capacity is especially high in developing nations, where resources are limited and cannot be invested in infrastructure cybersecurity and professional training. In even the most technologically developed jurisdictions, law enforcement agencies are faced with a challenge of keeping up with the ever-changing techniques of cyber-criminals, such as utilizing anonymization networks, encryption, malware and automated attack-tools (Amoo et al., 2024). The speed and robotization of cybercrime contribute to the widening of the enforcement gap since cybercrimes have the potential to cause extensive damage even before the law enforcement machinery has been deployed.

The other notable hurdle is the alignment of the services of the government with those of the business world. The important evidence is usually stored by Internet Service Providers (ISPs), cloud service providers, financial institutions or technology companies. Cooperation is necessary, but it is complicated by business privacy regulations, legal restrictions and commercial concerns (Lasopoulou, 2025). The timely and legal access to data cannot be negotiated without law authority

and general operational trust, which might be insufficient when it comes to cross-border negotiations.

There are additional barriers of anonymity and obfuscation technologies. VPNs, Tor networks, proxy servers and botnets are the tools that allow perpetrators to obscure their identity and geographic location. Police forces are seriously challenged with the inability to track criminals, assign blame and connect online actions to specific persons (Grochmal, 2025). These technical barriers are inconsistent with the traditional principles of investigation and demand advanced technologies such as network analysis, malware reverse engineering and cryptocurrencies tracking.

Lastly, artificial intelligence (AI)-aided cybercrimes create new dilemmas in enforcement. AI software is capable of independently writing malware, spear-phishing and deepfakes and in many cases is dynamically modified, which allows it to pass as such. This development is blurring the distinction between human and machine agency and making the question of criminal responsibility more difficult as well as the investigative approach (KAN, 2024). The law enforcement should employ hybrid strategies in order to curb these problems that incorporate the old way of investigators with modern technical knowledge, international collaboration and partnerships between the government and the businesses.

Overall, enforcement and investigative issues highlight how the current criminal justice frameworks are limited in dealing with cybercrime. Successful counteractions involve expenditure in technical ability, process change, cross-agency cooperation and active international participation to adopt the naturally borderless and high-tech digital crimes.

4. Comparative Legal Approaches

The challenge of cybercrime is global and therefore various legislations have been taken to deal with it as a result of differences in the legal traditions, the priorities of policies and technological abilities of different countries. The evaluation of major jurisdictions shows convergences and differences in dealing with the digital offenses, which can help clarify the ways of harmonizing the laws.

4.1 United States

Computer Fraud and Abuse Act (CFAA) is the federal law that forms the basis of cyber crimes in the United States. The CFAA is a criminal law that was enacted in 1986 and amended several times and criminalizes unauthorized access to computer systems, data theft and damaging the computer systems (Wilneff, 2023). The U.S. law emphasizes the application of the fault-based approach that requires demonstration of intent or knowledge, yet the scope of an unauthorized access has been a subject of controversy and has been applied haphazardly when the case was associated with a terms-of-service violation or automated scraping of data (Thomas, 2023). Besides the federal laws, state laws also deal with the problem associated with cybercrime including identity theft, online harassment and online impersonation, which forms a stacked legal system.

4.2 European Union

The European Union is more harmonized and regulatory. The criminal liability of the illegal access, interference and spreading of malware is criminalized by the Directive on Attacks against information systems (2013/40/EU) and NIS2 Directive (2022) strengthens cybersecurity responsibilities of operators of critical infrastructure (Braschi, 2025). The EU law balances criminals' punishment with compulsory reporting, risk control and prevention practices, which represents a proactive and technology-sensitive type of regulation. The EU system also focuses on cross-border collaboration with Europol and mutual judicial decision recognition, minimizing the jurisdiction conflict.

4.3 United Kingdom

The computer misuse act of 1990 (CMA) is the main law that has been utilized to criminalize unauthorized access to computer systems, unauthorized data manipulation and damage-inducing offenses in the United Kingdom (Khadam et al., 2023). The scope of the CMA has been broadened lately to include ransomware, phishing and other new cybercrimes. The UK law also places an importance on the investigation of law enforcement agencies and incorporates the integration of the cooperation of the private sector, which is a pragmatic approach that entails the integration of substantive criminal law and procedural flexibility.

4.4 China and Russia

Sovereignity-based cyber regulation is most clearly seen in the example of China and Russia, where the sovereign state is prioritized to control of the digital infrastructure, cyber-related activities and localization of data. In China, the Cybersecurity Law (2017) and its amendments criminalize hacking, online fraud and data breaches and place severe responsibilities on the network operators (Creemers, 2023). The Russian political system also has a similar legal system whereby there are substantive prohibitions as well as wide scope of surveillance and state monitoring. Though these solutions improve the ability of states to counter cyber threat within their borders, they do not comply with the international standards of collaboration across border, privacy and international due process.

4.5 Comparative Insights

Comparative analysis identifies a number of trends:

1. A majority of jurisdictions are currently realizing the need to have cyber-specific criminal provisions.
2. Fault-based liability is predominant, but there are very few situations where strict liability is used.
3. Coherence of procedural regulations, especially on the area of cross-border evidence gathering and cooperation is not yet fully established.
4. The models that are sovereignty-focused are likely to be incompatible with technology-neutral models or cooperative models across borders.

The lessons learned about these comparative aspects are the importance of cross-border collaboration, the modernization of traditional doctrines and the need to have a flexible, but stable approach to management of cybercrime in the global digital environment.

4.6 Harmonization Efforts and International Cooperation

Cybercrime is transnational and requires collaboration among countries in jurisdictions and harmonization of legal provisions. Unless there are coordinated actions, offenders will take advantage of discrepancies in the legislation, the powers of investigation and enforcement without compromising the effectiveness of criminal justice systems in any part of the world.

4.6.1 Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime (2001) of the Council of Europe is the most powerful international tool to harmonize the law on cybercrime (Buçaj & Idrizaj, 2025). It also defines cyber-crimes in common, sets procedural steps of investigation and supports international work on the issue with such mechanisms as expedited data-sharing and mutual legal assistance. Although it is mainly a Council of Europe initiative, the convention has gotten non-European states to adopt it, such as the United States, Japan and Australia. The Budapest Convention focuses on harmonization of substantive law, jurisdictional regulations and evidence management across the border, which gives an IL normative framework to those states interested in updating cybercrime laws.

4.6.2 OECD and Digital Security Principles

The Organisation for Economic Co-Operation and Development (OECD) is used to supplement harmonization in the treaty-based effort using soft-law means. In 2015, the OECD published its recommendations on digital security and privacy that inspire member states to take a risk-based approach, foster partnership between the government and the private sector and require standardization of cyber incidents reporting (Johnstone, 2023). Non-binding, but with an impact on the domestic legislation, judicial interpretation and corporate compliance, such principles help to create a consistent and international approach towards cybersecurity and cybercrime prevention.

4.6.3 UN Cybercrime Initiatives

Cybercrime has been identified as a global governance issue that has gained a lot of attention by the United Nations. Although a binding international treaty on cybercrime is still under negotiation, capacity-building, law enforcement training and information exchange are encouraged by UN legislations, such as resolutions of the General Assembly and the programs of the Office on Drugs and Crime (UNODC) (S. H. Khan et al., 2024). UN activities are focused on capacity building in the developing world where the gaps in technical skill and investigative capabilities are very important in determining the success of the international partnership. 8.4 Regional Cooperation and Agreements.

4.6.4 Regional Agreements and Cooperation

Harmonization is also achieved through regional mechanisms. There are directives grouped in the European Union, including the NIS2 Directive, the Cybercrime Directive, which create binding standards of cybercrime and enable judicial co-operation (Kamara, 2024). The cyber norms of the ASEAN and the cybersecurity plans of the African Union are aimed at coordinating legislative and investigative actions inside their respective areas, but these are not completely enforced. These regional projects complement international systems and offer a platform of operation on joint investigations, sharing information and capacity building programs.

4.6.5 Challenges and Future Prospects

In spite of all this, there are still major barriers. The major cyber powers such as China and Russia are not signatories to the Budapest Convention and place the state sovereignty above international collaboration. There remain conflicting legal definitions and procedural powers which do not align with each other, as well as privacy protections, as impediments to effective cross-border enforcement (Matei, 2024a). Going forward, hybrid approaches involving binding multilateral treaties, regional cooperation and soft-law tools could be the best way through to ensure that national law systems align with the global nature of cybercrime.

4.7 Policy and Legal Reform Recommendations

Considering such a fast development of cybercrime and the weaknesses of the traditional criminal law, policy and legal changes are necessary to support the enforcement, increase the collaboration of the countries and guarantee the rights protection in the electronic space. The subsequent suggestions will help to resolve substantive and procedural gaps.

4.7.1 Hybrid Digital-Specific Criminal Law

States ought to think of implementing hybrid forms of criminal law that would preserve the basic tenets of the traditional law, but include digital-specific clauses (Heine & Quintavalla, 2024). These frameworks would explicitly categorize cyber-crimes, differentiate between direct and indirect cyber harms and offer specific liability regulation to automated systems, bots and AI-perpetrated actions. This strategy strikes a balance between technological neutrality and the precision required and reduces the ambiguity as much as it is possible to ensure digital conduct is dealt with effectively.

4.7.2 Strengthening International Cooperation

More effective cross-border collaboration is essential to fighting cybercrime. The states are to ratify and enforce such instruments as the Budapest Convention and encourage regional and bilateral ones to exchange evidence quickly, conduct joint investigations and extradite offenders (Matei, 2024b). Capacity-building in the developing nations, especially technical skills, investigative infrastructure and harmonization of laws should be invested in to stop safe havens of cybercriminals.

4.7.3 Updating Procedural Powers and Standards

The procedural level reform should focus on securitizing the digital evidence and its collection, preservation and admissibility (M. N. I. Khan & Ahmed, 2025). The protocols in chain of custody, forensic examination and validation of evidence need to be internationally agreed upon. Laws have to balance between the rights to privacy, due process and protection of data and the investigative capacities without causing inadequacies in the enforcement procedures.

4.7.4 Enhancing Cyber Forensic and Investigative Capacity

States ought to form specialized Cyber Forensic teams and support to train law enforcer, prosecutors and judiciary (Gupta & Lunia, 2024). Public -private partnerships with technology firms, security vendors and academia can also be made to aid in real time monitoring and threat intelligence and technical support of an investigation. This enables the legal institutions to remain abreast with the rapidly emerging cyber threats.

4.7.5 Promoting Public Awareness and Prevention

Preventative measures such as education on digital literacy, cyber security and promoting responsible online conduct are vital adjuncts to legislation (Elrayah & Jamil, 2023). Communal education results in reduced prone-ness to computer-related felony, augmented police work and citizen collaboration, elevated responsibility with regard to computers that has a total contribution toward deterrence (and resilience) at the national level. These policy and legal changes can assist the states in modernizing the old connection between criminal law and crimes of the digital era. This and other reforms besides enhancing the effectiveness of enforcement provide more certain guidance of industry and encourage the international collaboration in a borderless cyber world.

5. Conclusion

The new digital technologies transformed the criminal environment, preconditioning the emergence of offences which are not tied to national borders, exploit the shortcomings in the technological security and challenge traditional types of criminal law. Cybercrime sheds light on the conceptual weaknesses of concepts as actus reus, mens rea, causation and jurisdiction and offers practical issues with acquisition of evidence forensic investigation and implementation. Digital crimes are transnational as well as automated, thus disturbing the territoriality of the crime and the historical beliefs on human agency and due process. An international and comparative analysis reveals that despite the fact that national legislations have progressively adapted to address cybercrime, several distinctions exist in defining and procedural regulations, investigative authority and cross-border collaboration modalities. Attempts to develop uniformity, e.g. the Budapest Convention, OECD rules as well as regional solutions are useful frameworks but are still incomplete and unequally implemented. The sovereignty approach, the capacity-capacity gap approach and the various approaches based on legal traditions make it tricky to develop a coordinated global response.

Cybercrime requires a multi-pronged approach to be regulated. This involves integrating old rules of the criminal law with the new rules of the digital world, enhancing international collaboration, updating the powers of the procedures, enhancing the forensic and investigative capabilities and encouraging the raising of awareness programs by the population. Through these changes, the states will be able to regulate the requirements of a dynamic digital environment along with the requirements of due process, legal predictability and preserving human rights.Ultimately, the field of cybercrime is a technology and legal issue. It needs to be characterized by bending, cooperative strategies. The development of legal systems should continue to adopt new forms of digital harm, as well as ensure that the pursuit of justice continues to be viable in a more integrated and technological world.

6. References

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), 205–217.

Braschi, S. (2025). The new EU Directive on combating violence against women and domestic violence. *Zeitschrift Für Die Gesamte Strafrechtswissenschaft*, *137*(2), 425–442.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, *46*(4), 189–206.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024–2025024.

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145.

Elrayah, M., & Jamil, S. (2023). Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness. *International Journal of Cyber Criminology*, *17*(2), 166–187.

Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal*, *38*(1), 29.

Gompert, D. C., & Libicki, M. (2023). Towards a quantum internet: Post-pandemic cyber security in a post-digital world. In *Survival february–march 2021: A house divided* (pp. 113–124). Routledge.

Graham, A. (2023). *Cybercrime: Traditional problems and modern solutions*. Open Access Te Herenga Waka-Victoria University of Wellington.

Graham, R. S., & Smith, S. K. (2024). *Cybercrime and digital deviance*. Routledge.

Grochmal, A. B. (2025). *Challenges Faced by Law Enforcement Collecting and Using Digital Evidence in Cybercrime Investigations*. Marymount University.

Gupta, J. K., & Lunia, U. (2024). Cyber Crime and the Challenges of Prosecution and Prevention. *Issue 4 Int'l JL Mgmt. & Human.*, *7*, 1038.

Heine, K., & Quintavalla, A. (2024). Bridging the accountability gap of artificial intelligence–what can be learned from Roman law? *Legal Studies*, *44*(1), 65–80.

Heyndels, S. (2023). Technology and neutrality. *Philosophy & Technology*, *36*(4), 75.

Holt, T. J. (2019). *The human factor of cybercrime*. Routledge London.

Hussain, S., Ashraf, S., Al Hamadi, H., & Abideen, Z. U. (2023). A Critical Analysis on Cybercrimes. *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1–7.

Irshad, E., & Siddiqui, A. B. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal*, *24*(1), 43–59.

Johnstone, I. (2023). Organisation for Economic Co-operation and Development (OECD). *Yearbook of International Environmental Law*, *34*(1), yvae026.

Kamara, I. (2024). European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research*, *37*(5), 1441–1460.

Kan, C. H. (2024). Criminal Liability Of Artificial Intelligence From The Perspective Of Criminal Law: An Evaluation In The Context Of The General Theory Of Crime And Fundamental Principles. *International Journal of Eurasia Social Sciences/Uluslararasi Avrasya Sosyal Bilimler Dergisi*, *14*(55).

KAUR, G., & DHAWAN, A. (2024a). *Laws of electronic evidence and digital forensics*. PHI Learning Pvt. Ltd.

KAUR, G., & DHAWAN, A. (2024b). *Laws of electronic evidence and digital forensics*. PHI Learning Pvt. Ltd.

Khadam, N., Anjum, N., Alam, A., Mirza, Q. A., Assam, M., Ismail, E. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, *9*(12).

Khan, M. N. I., & Ahmed, I. (2025). A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01–29.

Khan, S. H., Zakir, M. H., Tayyab, A., & Ibrahim, S. (2024). The role of international law in addressing transnational organized crime. *Journal of Asian Development Studies*, *13*(1), 283–294.

Lasopoulou, V. (2025). *Cloud security and privacy*. Πανεπιστήμιο Πειραιώς.

Matei, G. I. (2024a). Cross-Border Data Sharing and Sovereignty: Reactions of Non-EU Countries to Article 32 of the Budapest Convention. *Law and Economy*, *3*(9), 1–8.

Matei, G. I. (2024b). Cross-Border Data Sharing and Sovereignty: Reactions of Non-EU Countries to Article 32 of the Budapest Convention. *Law and Economy*, *3*(9), 1–8.

Metaxakis, E. (2023). Ratifying an international treaty: Is it enough?(Shortcomings of the ratification of the Budapest Convention by Greece). *International Cybersecurity Law Review*, *4*(4), 451–470.

Péter, F. (2023). The history of cybercrime legislation and major achievements. *Journal of Eastern European Criminal Law*, *01*, 26–35.

Salimi, F. (2024). *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*.

Shami, A. Z. A., Saleem, M., & Ashraf, J. (2025). Cybercrime And Digital Evidence: Investigating The Challenges And Opportunities In Prosecuting Cybercrime And Handling Digital Evidence. *Research Consortium Archive*, *3*(2), 401–411.

Shurson, J. (2023). *Rethinking Comity: Resolving Conflicts in Transnational Digital Investigations*. Queen Mary University of London.

Smith, R. G., Sarre, R., Chang, L. Y.-C., & Lau, L. Y.-C. (2023a). *Cybercrime in the pandemic digital age and beyond*. Springer.

Smith, R. G., Sarre, R., Chang, L. Y.-C., & Lau, L. Y.-C. (2023b). *Cybercrime in the pandemic digital age and beyond*. Springer.

Solove, D. J. (2025). Notable Privacy Books: A Journey Through History. *Available at SSRN 5277793*.

Stoykova, R. A. (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, *55*, 106040.

Thomas, A. J. (2023). Exceeding Authorized Access Under the CFAA. In *The Open World, Hackbacks and Global Justice* (pp. 211–261). Springer.

Wall, D. S. (2024a). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Wall, D. S. (2024b). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Wilneff, L. (2023). “So” what? Why the Supreme Court’s narrow interpretation of the computer fraud and abuse act in Van Buren v. United States has drastic effects. *Loyola University Chicago Law Journal*, *54*(5), 1.

Wu, L., Peng, Q., & Lembke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. *International Journal of Cybersecurity Intelligence & Cybercrime*, *6*(1), 5–28.

Xiao, G. (2023). *Data Misappropriation*.

Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, *28*(1), 21–44.