UCP Journal *of* Law & Legal Education
Vol. 3, Issue 2 (January – June 2025)

Enhancing Legal Frameworks to Address Cybercrime in the Digital Age: A Critical Perspective

Faisal Awais*

Abstract

Digital technology has progressed so fast that it delivers new possibilities, but also supports more sophisticated cybercrime. The present paper scrutinises the efficiency of the existing legal frameworks in working with cybercrime. It applies a qualitative research approach through doctrinal and comparative research. It looks into ratified instruments that address cybercrime, like the Budapest Convention and national laws of different countries, such as Pakistan's Prevention of Electronic Crimes Act (PECA) 2016, to determine their sufficiency in targeting the global and multifaceted nature of cybercrime. Among the most significant issues faced hence identified by the study are the complexities of jurisdiction, the alarming rate of technological evolution that exceeded legal evolution, and tensions between internet security and human rights, especially in terms of privacy and freedom of expression. The research points to the gaps in the established legal framework and emphasises the changes using the comparative analysis of cases and case studies. The paper also suggests that there should be an increase in legislative efforts, law enforcement practices and systems, global collaboration, as well as collaborations between governments and businesses. This is also critical in ensuring that human rights are incorporated into the cybersecurity plan to catalyse security and personal liberties. The study also has practical policy implications that can be implemented by policymakers to close regulatory gaps and increase the agility of legal frameworks. The study can fix existing gaps in the literature, source of policymakers, legal practitioners and scholars with a broader comprehension of the rapidly evolving field of cybersecurity.

Keywords: Cybercrime, Digital Technology, Budapest Convention, PECA 2016, Cybersecurity, Human Rights.

***Lecturer & Quality Circle Head, Faculty of Law, Superior University, Lahore. email: faisal.awais@superior.edu.pk

Article History: Received: 05 May 2025; Received in revised form: 07 August 2025; Accepted: 08 October 2025.
Available online: 20 October 2025
DOI: https://doi.org/10.24312/ucp-jlle.03.02.533

Introduction

Over the years, contemporary societies have experienced a major shift in the 21st century owing to advancements in digital technology. These developments have transformed the means of communication, business, governance and education; changed our lives and interactions. These advancements or technological changes have led to progress and connectivity, albeit increased risk of crime in society. The use of digital systems in crime has become a dominant problem, affecting individuals, corporations, and government institutions (Wall, 2007).

Cybercrime takes different dimensions, such as hacking of finances, ransomware, cyberstalking, and so on, which jeopardise vulnerable groups like children and convey disinformation. The statelessness of cybercrime causes complications to the legal system since the evildoers can use the connectedness of the internet to outsmart the law enforcement capacity. Hacking activities are usually based in a single location and unleashed on their victims in several jurisdictions, thereby making the ordinary territorial laws inactive (Brenner, 2010).

International law systems such as the Budapest Convention on Cybercrime (Council of Europe, 2001) and various United Nations initiatives have still grappled with tackling cybercrime, with the rate of technological change way higher than the one that the regulatory regimes can manage. These systems were supposed to fight the conventional crimes committed physically, and thus, controlling the digital offences is challenging. Issues, like anonymity of criminals, legal problems of transboundary investigations, and fast-changing technology, allow offenders to avoid detection. This brings about a big gap in regulation, undermining efforts to stop and counter cybercrime (Goodman, 2015).

The developing nations, such as Pakistan, have greater impediments to counter cybercrime as they have less money, less technology-savvy capability and a lack of awareness among people. The Prevention of Electronic Crimes Act (PECA) 2016 was enacted as the main body of law to deal with digital crimes. Nevertheless, its implementation has already presented several problems, due to jurisdictional ambiguity, and issues related to the politicisation of the legislation to an authoritarian end (Zahid, 2024). Pakistan's legal

mechanisms and those of several other states are significantly restrained that they have been characterised by imprecise jurisdiction boundaries, whereas technology advances at a faster pace than changes in law and security measures, on occasion infringe on human rights. Budapest Convention on Cybercrime and UN initiatives must be evaluated to determine their success at this point, as they already require more effective mechanisms strengthening international cooperation, enforcement, and data sharing. Addressing the respective gaps presents the only viable way forward to build a coherent international response capable of managing emerging cyber threats in a proper manner.

Literature Review

The digital revolution has changed the world irreversibly and introduced new opportunities for criminal exploitation. One of the main features of cybercrime is its transnational nature, technological sophistication and variety. Researchers contend that cybercrime is distinct and unique from conventional crime since it is immaterial to an extent that it is grounded on digital architecture and has no apparent jurisdiction (Brenner, 2010). Cybercrime grows far faster than the formulation of law. Developments in technology, including the possibility to remain anonymous on the internet, enable perpetrators to be ahead of the legislation (Goodman, 2015). Moreover, the fact that cybercrime is borderless restricts the jurisdiction rights and requires cross-national collaboration to prosecute criminals (Clough, 2015).

Adopted in 2001, the Budapest Convention on Cybercrime is the most comprehensive international agreement dealing with cybercrime. It offers the legal base concerning the equivalent laws of different countries, collaboration between countries and standard investigations (Council of Europe, 2001). Nonetheless, the participation of major regions like China and Russia, which are yet to become a part of the convention despite being faced with omissions regarding sovereignty and policies, has reduced the efficacy of the convention (Chen, S., 2023). Several resolutions and reports on cybercrime have been presented by the United Nations in response (United Nations Office on Drugs and Crime, 2020). Nevertheless, despite all those efforts, academics emphasise the scattered way of the UN to address the issue, and the lack of

enforcement power, and an excessive reliance on consensus is a detrimental factor (James, J.I., & Gladyshev, P., 2016). The international efforts are more concerned with the necessity of united efforts in strengthening the legal structure and cooperation.

The Prevention of Electronic Crimes Act (PECA) 2016 is the main act in Pakistan to manage and control cybercrime. Despite covering the most important topics of unauthorised access and stealing data, the implementation of PECA has not taken place without difficulties. The legal community has voiced the issue of unclear language and the possibility of the law overstepping the right to express their views and the right to protest (Zahid, 2024). Impediments such as the lack of trained personnel to deal with the recent methods of cybercrime also affect law enforcement agencies in charge of cybersecurity. In order to deal with such challenges, international cooperation and the involvement of public-private partnerships are compulsory.

The deployment of security versus the protection of human rights, especially the right to privacy and the right to free speech, has been the key issue in combating internet crimes (United Nations, 2013). Studies show that the oversimplification of cybercrime legislation by governments can lead to the infringement of human rights (Deibert, 2018). Thus, cybersecurity legislation should focus on human rights by making the policy of protecting individuals more transparent and the power to take action more responsible to ensure individual safety (Land, 2019). Cyber threats have necessitated the need for a public-private partnership to adequately deal with them. It has been observed that the private enterprises with their elaborate digital framework contribute significantly to the identification and prevention of cybersecurity threats (Kshetri, 2018). Lawful interrelationships must be designed to develop trust and share data among stakeholders.

Studies prove that countries such as Estonia and Singapore have undertaken effective legal and institutional developments to fight cybercrimes (Yeo-Moriuchi, 2023). Estonia has its national defence policies which encompass cybersecurity, and the rate of citizens is trained about possible threats, besides preparing workers against the eventuality of cybersecurity issues (Czosseck et al., 2011). The 2018 Cybersecurity Act in Singapore will require the stakeholders to play specific roles in battling cybercrime (Yeo, 2020). Such instances back up the reasoning that it is necessary to

have up-to-date laws, international cooperation, and training to tackle the changing face of cyber threats. According to James, J. I., & Gladyshev, P. (2016), nations are supposed to conform to international norms and work together internationally to come up with security frameworks that will guard human rights.

Brenner (2010) and Goodman (2015) thoroughly examine both global cybercrime trends and their international impact in their research. Research studies mainly concentrate on advanced nations because they overlook developing countries' particular cybersecurity challenges, particularly in Pakistan. Most studies about the Budapest Convention as a global legal tool examine European nations, but researchers usually omit to evaluate its applicability to Pakistan and other countries that did not sign the agreement.

Researchers (Zahid, 2024) criticise PECA 2016, yet an extensive review is missing to evaluate if this law meets international criteria and protects Pakistan from present-day cyber threats. Existing studies split cybersecurity knowledge from human rights analysis when creating legal frameworks, even though Land (2019) showed this approach needs improvement.

Research Methodology

This work is based on qualitative research aimed at exploring the problem of the control of cybercrimes on the basis of legal regulations in various countries. The study methodology will enable the author to review the official papers, law, and judgments made in courtrooms to evaluate the weaknesses and strengths of existing law enforcement mechanisms. It will be used in primary sources (the Budapest Convention, the Prevention of Electronic Crimes Act (PECA) 2016 in Pakistan), and secondary sources (academic works as well as reports of international organisations).

The study takes a doctrinal form as it examines literary writings and covenants, demonstrating legal texts and treaties. A comparative research approach is also implemented to analyse the manner in which various nations address cybercrime. Cyber-attacks are discussed to explain why the current regulations will not work and to point out why reforms should be carried out. The study focuses on the effectiveness of the existing legislation, the way in which various countries investigate the cases of cybercrime, the

technological transformations that are necessary, and how the legal regulations are adopted concerning the changing threats.

The study uses Pakistan as the case study to understand how the local laws can conform to international standards, even though it mainly focuses on international agreements. In the analysis, the shortcomings confronted by the surging technology and research resources have been realised.

The proposed methodology would offer viable policy recommendations to policymakers, practitioners, and researchers to enhance the efficacy of laws and mitigating measures established to contain cybercrime in the new digital era.

The Need for Stronger Legal Frameworks in Cybercrime Regulation

The high rate of embracing digital technologies has brought opportunities for innovation, as well as more advanced cybercrime methods. The current legal systems that mostly focus on solving conventional criminal activities within the offline environment are simply failing to meet the challenges of cybercrime within the digital world (Brenner, 2010). The enhancement of the legal means to fight against cybercrime is of utmost importance to proceed with technological progress without letting it affect the integrity of the online space and the welfare of people negatively.

The other strong threat is that cybercrime is transnational. Conventional crimes are generally limited to a certain jurisdiction; cybercrimes have the potential of crossing the border lines, with criminals in one nation ending up attacking users in another (Wall, 2007). Therefore, the legal machinery, both domestically and internationally, should be enhanced so that criminals cannot take advantage of the jurisdictional boundaries between states to get away with the crimes (Goodman, 2015). As an example, the Budapest Convention on Cybercrime (Council of Europe, 2001) offers a structure of international cooperation in addressing the topic of cybercrime, laying down laws, the standards of evidence sharing, and interstate criminal execution.

The future of the field in question is a very important part of strengthening legal frameworks because it deals with novel technological trends and challenges. Cybercrime constantly develops, and some of the threats include ransomware, AI-

facilitated attacks, and the use of the dark web (Bada & Nurse, 2020). Such trends render the traditional legal systems even more difficult to keep up with (Kshetri, 2018). The swift changes in the technological and cyber threat environment necessitate that legislators continually modify and revise existing laws to govern emerging issues adequately. Not doing so may generate loopholes in the legislation, and people and organisations will become exposed to excessive use of their data by cybercriminals.

Laws concerning cybersecurity should be developed to protect the subjects against such online hazards, protecting their basic human rights, such as privacy and freedom on the web (Zahid, 2024). Nonetheless, not all cybercrime laws are appropriate. Certain measures undermine the right to privacy among citizens, where lawmakers sanction the ability to retrieve personal information without the necessary tracking (Goodman, 2015). The application of the existing laws is not effective enough in the fight against cybercriminals and to address the challenges of digital security (Zohar, 2019). Laws need to be updated to guarantee human protection during investigations on cybercrimes (Goodman, 2015). Ensuring that the security laws in a country like Pakistan are enhanced to deal with the rising cases of cyber-threats is important, especially with fewer resources to enforce the law and less manpower in terms of training in the country (Zahid, 2024). Although there is a legal framework towards combating the problem of cybercrime enshrined in the Prevention of Electronic Crimes Act (PECA) 2016, there exist operational issues as well as unclear laws, which create some difficulty in its enforcement. The enhancement of the network-based crime prevention also demands not only new legislation, but effective training of police officers and court workers as the executors of the specified regulations (Zahid, 2024).

Increasing legal protection of citizens to enhance the level of online safety is arguably the most relevant course of action, as it can be accomplished through the effective cooperation of both the technology companies and the public institutions (Zohar, 2019). Corporations, especially those in the technological sphere, will have to collaborate with governments to build stronger barriers against cybercriminals. Organisations are to ensure that they liaise with the government in developing comprehensive legal frameworks to deal with cybercrime and, in addition, build strong partnerships with all

the industries that are affected by cybercrime (Anderson et al., 2021).

A key to improving the work in the field of cybersecurity is devising more effective legal means to deal with cybercrime. Expanding digital business with the associated improvement in public safety is possible through the betterment of the legal framework and response systems. The strategy is useful in making sure that there are gains realised through the use of new technologies, and the threat caused by cybercrime is reduced.

Understanding Cybercrime in the Digital Era

In the contemporary era, cybercrime has become one of the greatest issues in the world. It includes an extensive variety of criminal manifestations enabled by digital technologies, such as financial fraud, assault upon national security, etc. This fact indicates the frailties of the utilisation of digital systems that are becoming more exposed to attacks by cybercriminals. As such, it is of paramount importance to gain certain levels of insight regarding the extent of cybercrime, its impact, and the equipment needed to deal with and avert such a menace successfully. As the technology continues to advance, cybercrime has taken a different identity and dimension. Contrary to traditional crimes, which are usually limited to geographical boundaries, cybercrimes allow infiltration of the open market of the internet, hence confusing as to jurisdiction and consequently prosecution. Cybercriminals are adopting more sophisticated methods of carrying out their illegal operations anonymously and with finer precision tools like encryption, artificial intelligence (AI) and the dark web (Clough, 2015). Such technological developments become an advantage to cybercriminals as they allow them to be more sophisticated in their operations, with larger-scale systems and networks becoming their targets.

In addition, cybercrime is no longer a local issue as it has now been organised to a greater level. It is not a rare occurrence when perpetrators act across several jurisdictions and attack financial systems, critical infrastructure, and individual users (Anderson et al., 2021). The ramified use of ransomware attacks is one of the brightest examples of the significant economic and psychological blow the victims, companies, governments, and individuals may face as a result of cybercrime (Lowry, 1951).

Cybercrime can be classified into several distinct categories, each posing unique threats (Bada & Nurse, 2020).

i. **Financial Crimes:** There are fraud, identity theft, and violations relating to cryptocurrency.
ii. **Attacks on Critical Infrastructure:** Cyberattacks on Critical Infrastructure: Those targeting critical infrastructure for fear or impact via disruption of medical and other critical services.
iii. **Cyber Espionage:** Unauthorised access to sensitive information for political or economic gain.
iv. **Social Harm Crimes:** Cyberstalking, online harassment, and Child exploitation are examples of Social Harm Crimes.
v. **Information Manipulation:** Information Misinformation and Disinformation in a bid to manipulate public opinion.

Factors Facilitating Cybercrime

There are various aspects that have enhanced the speedy emergence of cybercrime. Firstly, it has become common that internet-enabled devices are everywhere, and this has given hackers a large and diverse group of people to exploit. These gadgets, from smartphones to laptops, enable connectivity, and hence people and organisations can be easily exposed to cyber hackers. Secondly, there has been easier access to the transnational flow of data, and this has facilitated criminal activities as cybercriminals can easily cross borders to execute crimes. The transnational characteristic of cybercrimes further makes it difficult to compensate through regulation, ensuring the prosecution of criminals, as laws and enforcement strategies often lag behind the digital world. Thirdly, most of the developing countries are faced with poor legislation and enforcement mechanisms that make them ill-prepared in the fight against cybercrime. Finally, the overall weakness of cybersecurity awareness by the general population contributes to the rise of the risk of people becoming victims of cyberattacks. Cybercriminals find it easy to attack many individuals without the right research on cybersecurity best practices, enhancing the total increase in cybercrimes (Zahid, 2024). Cybercrime is expected to cause the global economy to spend about 10.5 trillion dollars per year by 2025, mostly because of ransomware attacks, financial fraud, and

data breaches. Nonetheless, the financial ramification is only a part of the overall effects of cybercrime. Digital crimes also undermine confidence in digital systems, damage privacy, and insecurity permeates society with fear. All these problems make cybercrime a very difficult issue to combat (Morgan, 2020).

The current state of developing nations is most vulnerable to Cybercrime since these countries have minimal resources, technical knowledge, and infrastructure. These grey areas have embraced these digital systems quickly than they could develop the corresponding security infrastructure, thus giving the cybercrime operators a free hand. Inadequate legislation on cybersecurity, along with its lack of enforcement, means that, typically, numerous cybercrimes are not even reported to the police (Broadhurst, 2019).

Alongside the rise of cybercrime in the digital age, it can be argued that the issue must be addressed from a multidimensional perspective, incorporating technological, legal, and societal dimensions. Since cybercrime is expanding in scale and continues to be a global threat, the nature of cybercrime poses inherent threats that will necessitate international cooperation among countries, companies, and individuals. The underlying issues regarding cybercrime should be understood fully to combat this increasingly common menace. Such knowledge will be required to outline proper legal frameworks and combat the escalating crime rate through global collaboration practices.

Case Studies: Insights into the Legal and Practical Challenges of Cybercrime

Examples of cybercrime cases can provide valuable insights into the challenges faced by modern efforts and the effectiveness of current legal frameworks in addressing these crimes. These case studies reveal the character of cybercrime, the issue of burden of jurisdiction, and the ways in which the methods used by cybercriminals are increasingly involving the nature of a multi-faceted crime. The case studies below give a detailed example of how cybercrime affects the community globally.

WannaCry Ransomware Attack (2017)

The WannaCry ransomware attack is just one of the biggest cybercrime occurrences worldwide (Kshetri, 2018). Ninety-five percent of the websites infected by this attack included WordPress, and it was spread to over 200,000 systems around the world, up to 150 countries, encrypting users' data and demanding that a ransom be paid in Bitcoin. Healthcare systems, banks and governmental institutions, especially the National Health Service (NHS), suffered major disruptions. This exposed some serious jurisdictional issues. Although the US and UK intelligence have blamed a North Korean hacking group for the ransomware, no extradition treaties and international legal mechanisms made prosecution impossible. Governments and businesses throughout the globe recognised the need for better cybersecurity protocols, including regular software updates and backups. Existing laws to curb cross-border cybercrimes have become mere paper tigers, the case illustrated.

The Yahoo Data Breaches (2013-2014)

Yahoo has been the scene of a series of data breaches in the years from 2013 to 2014, impacting the personal information of over 3 billion user accounts (Wang & Park, 2017). Stolen names, email addresses and hashed passwords were among the breaches that were not even disclosed until 2016. The allegations of negligence led Yahoo to many lawsuits arising after the data breaches that greatly affected its worth once acquired by Verizon. The ethical doubt about data privacy rights, as to accountability, was also at stake when these breaches happened, especially regarding the accountability of the parties. In addition, the case brought out the issue of prosecuting state-sponsored hackers. Eight of the nine individuals, in linkage to the breaches, were ultimately indicted by the U.S. government and are believed to have ties with the government of Russia (Perlroth, 2021). However, the breaches could not have precipitated the adoption of the General Data Protection Regulation (GDPR) that was launched in Europe recently, which requires tighter measures towards data security and transparency.

Pakistan's Cybercrime Case: Digital Rights Foundation vs. PECA (2023)

To prevent the crime of cyber, Pakistan passed its Cybercrime Act known as the Prevention of Electronic Crimes Act (PECA), 2016. Nevertheless, controversies have erupted regarding the implementation of it with regard to freedom of expression and privacy rights (Perlroth, 2021). Digital Rights Foundation (DRF), one of Pakistan's premier human rights NGOs, filed petitions challenging some of the provisions of PECA. According to Zahid (2024), they argued that Section 20, which criminalises online defamation, was being misused to silence dissents and journalists. The challenges presented to legal and social policy by combating cybercrime emerge from this case. PECA has been particularly useful in addressing certain problems like online harassment, etc. The case led to a public debate on cracking the balance between cybersecurity and civil rights, and calls for amendments in PECA to avoid abuse.

Sheraz Khan vs. The State (2021)

With examination of the scope of jurisdiction for cybercrime cases under the Pakistan Provisions of Electronic Crimes Act (PECA), and the separation of trials, this case seeks to define the legal snares in the concept of cybercrime in Pakistan. The petitioner, Sheraz Khan, the petitioner, sought to invalidate PECA for criminalising the acts already criminalised under the Pakistan Penal Code, 1860 (PPC). The court held that, accused charged under PECA, and others, should not be tried at the same time. This decision also highlighted that cybercrime that occurs through information systems should be tried before the specialised courts established under PECA, even when the cybercrime overlaps with other offences defined under other laws. The court has indicated that a trial of cybercrimes and personal offences (such as cyberstalking, spamming, or spoofing) must be kept separate to avoid legal confusion and to ensure that the proceedings are in accordance with the correct legal frameworks. The case explains that there is a problem in the enforcement of cybercrime laws in an environment where various legal frameworks interconnect. Indeed, the ruling highlights the need for special courts to handle these particular

crimes, but it also demonstrates how laws can overlap and complicate prosecution.

Pakistan's Cyber Terrorism Case: Ismail Ijaz v. The State (2023)

The petitioner is Ismail Ijaz, who challenged a post-arrest bail granted to him in a charge under Sections 9, 10 and 11 of the Prevention of Electronic Crimes Act, 2016, for re-tweeting a message, which glorified a proscribed organisation, promoted cyber terrorism, and hate speech. The case explored the ambit of intent (mens rea) as far as cybercrimes were concerned, and in particular, could retweeting be considered as an intentional act to promote hate speech or terror. The court acquitted the petitioner of the charge of glorifying a proscribed organisation or advancing its interests since the State failed to establish material evidence that the accused was involved in glorifying a proscribed organisation or advancing its interests. The court held that just retweets alone do not demonstrate the required intent for the glorification of the organisation or the promotion of terrorism.

The Equifax Data Breach (2017)

Equifax, one of the largest credit reporting agencies in the U.S, had its data breach, which exposed sensitive information and social security numbers of more than 147 million people. Equifax was sued by various players, such as the Federal Trade Commission (FTC), which won a $700 million settlement, and came under regulatory fines. However, it also detailed the imperative for bordering data more appropriately (Gaglione Jr, G.S., 2019). Data security has proved to be a major lesson to the lawmakers, especially in the necessity of having stricter regulations. This has brought about a tussle over time as to whether strict federal-level data protection laws will be required to ensure the personal information of citizens is not subject to misuse and unauthorised accessibility.

The Silk Road Case (2013)

In the meantime, the dark web marketplace known as the Silk Road allowed illegal goods to be sold on the market, including drugs and weapons using Bitcoin (Gehl, 2018). Ross Ulbricht, the

site's founder whom was arrested in 2013 and subsequently convicted in 2015 of money laundering and conspiracy to commit computer hacking, among other counts. As far as the jurisdictional challenges are concerned, since the Silk Road operated globally, it was very hard for law enforcement agencies to successfully track transactions and users. A case such as this demonstrates the anonymity problems that the cryptocurrency and dark web pose. The conviction of Ulbricht was a significant legal and policy implication in the prosecution of cybercrime linked to the dark web. Moreover, it encouraged governments to make stronger controls with regard to transactions for cryptocurrencies and the monitoring of the dark web.

Legal Insights from the Case Studies

The jurisdiction of cybercrimes is a complex matter. The cases discussed above demonstrate the necessity to authorise jurisdiction in cross-border crimes through international treaties. With regard to legislative loopholes, such as the Equifax breach and Yahoo hacks, it is quite evident that strong data protection laws are necessary. These cases have indicated that there are many weaknesses in data security and that we are still in need of strong legislation in order to safeguard personal information and to make organisations responsible. The conflict between national security and individual rights is the most important problem in current cybersecurity laws. In these cases, there is a dilemma for policymakers to ensure good security while safeguarding individual liberties. These cases show how the lawmakers need a fine line when coming up with laws that will safeguard the citizens against the infringement of their rights.

Secondly, the growing use of cryptocurrency in criminal activity demonstrates the difficulty of regulating digital money as far as cybercrime is concerned. Cryptocurrencies should be controlled and checked in order to exclude their use in dark web operations. Cryptocurrencies, like Bitcoin, ensure anonymity, thereby making them an ideal way of settling illegal payments online on websites like Silk Road. Nevertheless, regulatory oversight has completely failed to check the activities of cybercriminals. Finding the right balance between guarantees of

financial privacy to legitimate users and the avoidance of criminal activity is vitally important for beneficial regulation.

Factors Contributing to Cybercrime

During the era of technology, the internet has become one of the greatest threats to security in the world, with its capabilities of causing great damage. These emerging criminal activities venture into the world of computers, networks, and digital devices, which have become either a tool, a target or a place for carrying out criminal activities. The following part explores the major impediments and aspects that lead to simplistic and partisan debate on numerous cybercrime problems.

Technological Advancements

Cybercriminals always use technology as tools and methods. The fact that there is use of advanced malware, ransomware and possibilities of phishing techniques combined with the reach of the internet across the planet makes it difficult to combat cybercrime. Different technologies, like VPNs and networks that anonymise (such as Tor), make cyber criminals' identities harder to find. Malware is also advanced as there are many common tools such as ransomware is one of them, and cybercrimes have become more severe and frequent.

Lack of International Cooperation and Jurisdictional Challenges

Many cybercrimes transcend borders and create complicated scenarios for law enforcement, along with jurisdictional challenges, making international cooperation extremely necessary. The efforts to combat cybercrimes taking place across jurisdictions are fragmented. In the absence of such efforts, the courts and law enforcement agencies continue to be impaired in exercising their cognisance in different instances due to jurisdictional conflicts and legal incompatibility (Button et al., 2025)

To evade justice, cybercriminals operate in countries with limited legal cooperation or no extradition agreements. The process

of obtaining the necessary legal instruments for cross-border cooperation is slow and cumbersome (Brenner, 2010).

Legal Gaps and Inadequate Legislation

Legal frameworks currently in place are not enough to cover the complex nature of today's cybercrime. Some of these are legislative gaps, and others are just outdated laws that make it difficult to ever prosecute cyber criminals effectively because these laws fail to respond to the latest forms of cybercrimes, such as hacking, data breaches, and identity theft (Brenner, 2010)

Most countries do not have comprehensive laws on major aspects of cybercrime, like hacking, online fraud and cyberbullying, which results in insufficient protection (Anderson et al, 2021).

Rapid Growth of Digital Platforms

As online platforms such as social media and e-commerce platforms grow, cybercriminals have also come up with new opportunities to exploit users. As social media is a prime target for cybercriminals, the common security lapses they tend to exploit include identity theft, phishing attacks and cyberbullying. To put it simply, the personal data stored online is incredibly vast, making users vulnerable to cybercrimes. There is an increase in online shopping and use of digital payments, which brings about the rise of fraud, payment diversion and other cybercrimes. Sensitive data will need to be protected from exploitation on secure platforms.

Low Cybersecurity Awareness

The absence of cybersecurity knowledge among users creates system vulnerabilities that help cybercriminals thrive. Internet users who fail to maintain good cybersecurity practices through password updates and two-factor authentication become easy victims of cybercriminals (Patane, Rakate, Ahire, & Sonawane, 2025). Small and medium-sized businesses face cybercrimes easily because they usually cannot afford robust cybersecurity protection.

Involvement of Organised Crime and State-Sponsored Actors

State-sponsored actors, together with organised criminal organisations, perform cybercrime with improved resources and better technical abilities.

Ransomware attacks and other extensive criminal activities become successful and more difficult to stop because cybercriminals form established criminal organisations (Patane, Rakate, Ahire, & Sonawane, 2025). Secondly, National governments also support certain cyberattacks as they aim to damage foreign infrastructure and steal confidential data, along with disrupting essential public services (Gehl, 2018).

Anonymous Payment Systems and Cryptocurrencies

The rise of cryptocurrencies, together with anonymous payment systems, created additional transaction channels for cybercriminals through simple and secure processes.

The use of Bitcoin and similar digital currencies enables users to perform transactions without traceable features, which prevents authorities from following the money trail. Drugs, together with stolen identities, find hiding places on dark web marketplace platforms which operate using cryptocurrencies.

Emerging Threats and Evolving Tactics

Cybercrime continues to develop by introducing new threats such as malware driven by AI vulnerabilities related to IoT (Internet of Things) devices and enhanced cyber terrorism capabilities. Cybercriminals use artificial intelligence to manufacture attacks with automated botnets for DDoS (Distributed Denial of Service) attacks as well as automated phishing schemes. Internet of Things (IoT) devices now exist as easy targets for cyberattacks because their growing numbers expose more attack surfaces (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015).

Cybercrime is a multidimensional issue that has many challenges as far as dealing with its impact is concerned. The combat against cybercrime is also challenged by new technologies emerging all the time, the expansion of cybercrime and its distribution all over the globe, and the legal regulation system's deficiencies. The fight

against these types of threats requires international cooperation, laws, and regulations as well as improved cybersecurity standards (Akhgar & Brewster, 2019).

Recommendations: Enhancing the Legal Framework to Combat Cybercrime in the Digital Era

With emerging cases of cybercrime every now and then, nations need to devise improved and elaborate mechanisms for curbing these crimes. The prevalent approach to combat cybercrime would be the continual updating of the regional rules and increased collaboration on the international level. This must incorporate capacity building and developing partnerships between the governmental organisations and the business corporations, as well as harnessing highly advanced technological equipment. Below is an in-depth exploration of these recommendations:

Strengthening Domestic Legal Frameworks

National cybercrime prevention requires countries to implement and improve their legal frameworks.

The implementations of cybercrime laws must remain neutral toward technological advances because they need to adapt to new digital crimes without restriction. Periodic legislative reviews need to happen for the efficient handling of new crime types such as cryptojacking and offences involving AI systems and deep fakes.

Singapore implemented the technology-neutral Cybersecurity Act of 2018, which enables quick responses to modern technical risks, according to James, J. I., & Gladyshev, P., 2016.

The criteria for data protection must be preserved because they stop identity theft and fraud attempts. Countries which lack strong data protection laws should establish their standards using the GDPR framework, which the EU currently operates.

According to Custers et al. (2019), research shows that the successful data protection frameworks are those which effectively cut down the occurrence of data breaches.

The legislative system needs to achieve equilibrium between digital security growth and protection of basic human rights, which include both free expression and privacy rights. A

disproportionate use of cybercrime legislation for monitoring civilians, along with the oppression of dissenting voices, leads to damaged public confidence in government management systems.

The Prevention of Electronic Crimes Act (PECA) in Pakistan requires modification to prevent digital misapplication while protecting citizens' rights (Iqbal et al., 2023).

Capacity Building for Law Enforcement and Judiciary

Specialised law enforcement agencies, together with competent judges, need to fight cybercrime efficiently.

Firstly, Public training sessions for law enforcement personnel and judicial officials and prosecution groups enable them to grasp digital examination techniques alongside cyber law procedures and official requirements. Secondly, the National Cyber-Forensics and Training Alliance (NCFTA), based in the United States, delivers workshops that provide contemporary knowledge to law enforcement agencies (James, J. I., & Gladyshev, P., 2016). Thirdly, establishing dedicated fight against cybercrime teams within police departments delivers the most effective results in cybercrime law enforcement. The units must consist of personnel who have expertise in IT and digital forensics, and cyber law.

Specialised units in cybercrime investigations greatly boost the investigational speed and efficiency, according to Goodman (2015). Last but not least, Protectors of forensic investigations need to allocate resources toward obtaining modern investigative tools, including blockchain analysis tools, together with artificial intelligence software to handle evidence acquisition and assessment.

Enhancing International Cooperation

The worldwide character of cybercrime demands that nations form alliances to fight this crime effectively.

The Budapest Convention on Cybercrime provides countries worldwide with a basis for unified legal systems in addition to international cooperation frameworks. A national alignment of laws provides a basis for international information-sharing among nations.

The evidence obtained through research demonstrates that when countries adopt common regulatory approaches, their

cybercrime prosecutions experience fewer conflicts pertaining to jurisdictional matters (Button et al., 2025).

Nations must establish diplomatic agreements which enable them to engage in extradition procedures and conduct common investigation operations together. Extradition conventions built exclusively for cybercriminals make it possible for borders to facilitate speedy judicial procedures.

According to Akhgar and Brewster (2019) treaties represent a crucial solution to solve jurisdictional gaps.

Real-time sharing of intelligence through collaborative systems enables countries to cut down their cyber threat response durations. In this regard, Cybersecurity Emergency Response Teams (CERTs) provide for successful collaboration in the European Union.

Promoting Public-Private Partnerships (PPPs)

The private sector should maintain control over vital infrastructure systems, along with digital network security functions, as its primary responsibility.

Organisations working together between the public and private sectors offer better threat intelligence exchange systems to address threats systematically.

Informative platforms such as Cyber Threat Alliance (CTA) show how partnership information sharing lowers system vulnerabilities (Anderson, 2021).

Both public authorities and private organisations need to create standard cybersecurity requirements which should target essential sectors, including healthcare and finance.

Effective cybersecurity guidelines emerged from the collaboration between the US National Institute of Standards and Technology (NIST) and industries.

Solicited tax breaks and subsidies help private companies to implement robust cybersecurity practices, which expand the overall digital safety realm.

Leveraging Emerging Technologies

New technology systems create multiple beneficial detection and prevention possibilities in cybercrime battles.

System analytics processed by AI machines check extensive quantities of data to track possible cyber risks during real-time operations.

The research by Thomas (2009) demonstrates how AI models effectively managed to inhibit ransomware intrusion attempts.

Similarly, Digital transactions become safer through blockchain because this technology builds security layers which prevent cybercriminals from altering electronic systems.

Public records and citizen identity protection become possible through governmental implementation of blockchain technology (Warikoo, A., 2014).

Raising Cybersecurity Awareness

To achieve cyber-resilience at the societal level, public education and awareness-building exercises must be implemented.

To establish a safer cybersecurity environment, the government needs to organise public information campaigns which teach citizens about protecting their information from threat groups and recognising fraudulent email attempts.

Research shows that general awareness programs lower phishing target accomplishment rates by 40% (Yong-mei, C., & Afzal, J., 2023).

Similarly, the process of teaching cybersecurity principles across every stage of education will build up citizens with digital proficiency skills.

Other countries should draw learning from Finland's approach to incorporating cybersecurity into its national curriculum.

Moreover, the government should participate in backing ethical hacking programs because these programs find security weaknesses in essential systems.

An effective measure to cope with cybercrime will involve cooperation between different stakeholders, which will enhance legal systems, technical capabilities, and operational models. Countries which follow the provided cybersecurity recommendations will place strong protective forces to handle the issues of the digital age. According to this, governments, private as well as international organisations, need to collaborate to provide a secure and trustworthy digital environment.

Conclusion

Modern technology has contributed a lot to the social, economic, and political aspects of society and catalysed growth and development. Nevertheless, it has also brought in the weak links that are used by cybercriminals, which bring the traditional law enforcement systems and law agencies into difficulty. As this paper has noted, cybercrime is a dynamic phenomenon and it has dynamic boundaries, changing relationships, and far-reaching impacts on society. Such advances in the law, as the newly implemented PECA in Pakistan or the Budapest Convention, are still inadequate. Legal, institutional, and technological structures, which are used to deter cybercrime, remain problematic, causing gaps in the defence against such crimes.

A number of crucial issues are recognised in the analysis. To begin with, cybercrime is not local but rather global and as such, it requires both international collaborations to house it. National boundaries are not barriers to the activities of cybercriminals. Second, the swift development of technology presents problems to the legislative system, making it challenging for governments and local law enforcement organisations to curtail threats that arise. Third, scarce funds, especially in developing nations, hinder the creation of sophisticated or strong cyber protection systems, thus making individuals and companies easy prey.

In order to counter these problems, the paper proposes the following policy recommendations: governments need to tighten up legal frameworks, undertake public-private partnerships (P3), build better foreign relations, and leverage Java's innovation opportunity, such as artificial intelligence and blockchain. Moreover, there is a necessity to develop the potential of law enforcement and justice, at the same time raising awareness of society regarding the comprehensiveness of cybersecurity.

This paper justifies the necessity of holistic treatment of cybersecurity as a combination of legal and technical aspects within society. It is the cooperation of political entities, businesses, and civic organisations only that could protect the benefits of the information revolution against the threats by new technologies. Global and regional initiatives that seek to fight the challenge of cybercrime can be upgraded to ensure that societies enjoy the use of

digital technology with reduced threats to citizens and organisational activities.

At last, future research is needed in new aspects, including quantum computing effects on information encryption, ethical issues in AI cybersecurity, and the participation of non-state adversaries in cyber warfare. This will facilitate the establishment of more proportional and advanced strategies to fight cybercrime, bearing in mind that technology and the modern environment are constantly changing.

References

Akhgar, B., & Brewster, B. (2019). *Challenges priorities and policies: Mapping the research requirements of cybercrime and cyberterrorism stakeholders*. Springer. Retrieved from https://nottingham-repository.worktribe.com/output/3774791

Anderson, R. (2021). *Security engineering: A guide to building dependable distributed systems*. Wiley. Retrieved from https://books.google.com.pk/books?hl=en&lr=&id=eo4Otm_TcW8C&oi=fnd&pg=PT14&dq=Anderson,+R.+(2021).+Security+engineering:+A+guide+to+building+dependable+distributed+systems&ots=gDIMBNcC5b&sig=PK40VAWi_Q30-JklgwzcECiE3kg&redir_esc=y#v=onepage&q&f=false

Bada, M., & Nurse, J. R. C. (2020). *Cybersecurity awareness campaigns: Why do they fail to change behavior?* Communications of the ACM, 63(2), 70–79. Retrieved from https://arxiv.org/abs/1901.02672

Broadhurst, R. (2019). *Cybercrime in developing economies: A case study of Southeast Asia*. Crime, Law and Social Change, 71(1), 47–65. Retrieved from https://books.google.com.pk/books?hl=en&lr=&id=Q9FGEAAAQBAJ&oi=fnd&pg=PA89&dq=Broadhurst,+R.+(2019).+Cybercrime+in+developing+economies:+A+case+study+of+Southeast+Asia.+Crime,+Law+and+Social+Change

&ots=0pLOGdiZrq&sig=oLB-S3vauL0rf-G-XcX88mgBQvw&redir_esc=y#v=onepage&q&f=false

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2025). *Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective.* Criminology & Criminal Justice, 25(2), 670-691. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/17488958221128128

Chen, S., Hao, M., Ding, F., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). *Exploring the global geography of cybercrime and its driving forces*. *Humanities and Social Sciences Communications, 10*(1), Article 15. Palgrave Macmillan. https://doi.org/10.1057/s41599-023-01560-x

Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press. https://books.google.com.pk/books?hl=en&lr=&id=3s13CgAAQBAJ&oi=fnd&pg=PR8

Czosseck, C., Ottis, R., & Talihärm, A. (2011). *Estonia after the 2007 cyber-attacks: Legal, strategic, and organizational changes in cybersecurity*. https://books.google.com.pk/books?hl=en&lr=&id=vub26dKsmpIC&oi=fnd&pg=PA72

Deibert, R. (2018). *Reset: Reclaiming the internet for civil society*. House of Anansi Press. https://cir.nii.ac.jp/crid/1970023484920448812

Gehl, R. W. (2018). *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P*. MIT Press. https://books.google.com.pk/books?hl=en&lr=&id=QzdmDwAAQBAJ&oi=fnd&pg=PR7

Gaglione, G. S., Jr. (2019). The Equifax data breach: An opportunity to improve consumer protection and cybersecurity efforts in America. *Buffalo Law Review, 67*, 1133. https://heinonline.org/HOL/LandingPage?handle=hein.journals/buflr67&div=34&id=&page=

Goodman, M. (2015). *Future crimes: Inside the digital underground and the battle for our connected world*. Anchor Books. https://cir.nii.ac.jp/crid/1970586434884166155

Iqbal, M., Talpur, S. R., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the challenges in Pakistan. *Siazga Research Journal, 2*(4), 273–282. https://journals-uoli.com/index.php/SRJ/article/view/35

James, J. I., & Gladyshev, P. (2016). A survey of mutual legal assistance involving digital evidence. *Digital Investigation, 18*, 23–30. https://doi.org/10.1016/j.diin.2016.06.004

Kshetri, N. (2018). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press. https://books.google.com.pk/books?hl=en&lr=&id=dPNWEAAAQBAJ&oi=fnd&pg=PP1

Land, M. (2019). Human rights and technology: New challenges for justice and accountability. *Annual Review of Law and Social Science, 15*, 1–20. https://www.annualreviews.org/content/journals/10.1146/annurev-lawsocsci-060220-081955

Lowry, O. H., Rosebrough, N. J., Farr, A. L., & Randall, R. J. (1951). Protein measurement with the Folin phenol reagent. *Journal of Biological Chemistry, 193*(1), 265–275. https://doi.org/10.1016/s0021-9258(19)52451-6

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybersecurity Ventures. https://cybersecurityventures.com

Patane, R., Rakate, V., Ahire, H., & Sonawane, S. (2025). Fraud detection in financial transactions using machine learning algorithms. *Anveshan*, 155. https://iccs.ac.in/assets/images/publication/Anveshan-2025.pdf#page=163

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing. https://ostromworkshop.indiana.edu/pdf/cyber-series/04-09-cyber-bookclub.pdf

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Thomas, N. (2009). Cyber security in East Asia: Governing anarchy. *Asian Security, 5*(1), 3–23. Taylor & Francis. https://doi.org/10.1080/14799850802611446

Trautman, L. J., Hussein, M. T., Ngamassi, L., & Molesky, M. J. (2020). Governance of the Internet of Things (IoT). *Jurimetrics, 60*(3), 315–352. https://ieeexplore.ieee.org/abstract/document/8795541

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press. https://books.google.com.pk/books?hl=en&lr=&id=DIMCEQAAQBAJ&oi=fnd&pg=PT7

Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. *Information Security Journal: A Global Perspective, 23*(4), 172–180. Taylor & Francis. https://doi.org/10.1080/19393555.2014.931491

Yar, M. (2013). *Cybercrime and society* (2nd ed.). SAGE Publications. https://www.torrossa.com/en/resources/an/5730571

Yeo-Moriuchi, K. J. (2023). *Human factor cybersecurity: Cybersecurity self-efficacy*. https://dr.ntu.edu.sg/entities/publication/423e3de1-f9c2-4d7c-bb0b-288ad7f74be7

Yong-mei, C., & Afzal, J. (2023). *Evaluating the impact of cybersecurity awareness programs on phishing susceptibility*. *Journal of Information Security Research, 12*(3), 145–158.

Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and criminal law in Pakistan: Societal impact, major threats, and legislative responses. *Pakistan Journal of Criminal Justice, 4*(1), 223–245. https://journals.centeriir.org/index.php/pjcl/article/view/102