THE JOURNAL OF RESEARCH REVIEW

P-ISSN: 3006-2632	E-ISSN: 3006-2640
Vol. 3. No. 01 (Jan-Mar) 2026	Page 454-466

https://doi.org/10.5281/zenodo.20716692

Cybercrime Legislation and Enforcement in the Twenty First Century: A Critical Analysis of Legal Frameworks, Operational Challenges, and the Balancing of Security with Civil Liberties

Humail Zainab	Advocate High Courts Pakistan, Email: humailzainab@gmail.com
Sidra Ilyas	Advocate High Court and Visiting Lecturer Law Department Hazara University Mansehra, Sidrakhan4079@gmail.com
Saira Ali	Assistant Professor, Department of Law, University of Haripur, Haripur saira.ali@uoh.edu.pk

Abstract: *With the explosion of connectivity via the internet, cybercrime has emerged as one of the most widespread and expensive security threats in today's society and will cost societies $10.5 trillion a year by 2025. This article examines cybercrime legislation and enforcement in the twenty first century in a comprehensive manner with the help of international law, criminology and public policy perspectives. This analysis starts from a detailed classification of cyber offenses based on three categories: crimes against cyber systems, crimes using cyber systems and crimes in cyber systems; and identifies the characteristics of cyberspace that challenge conventional territorial jurisdiction. The article examines critically the international legal landscape and compares the Budapest Convention of the Council of Europe with other regional instruments which have come into existence as well as with the proposed United Nations convention. In the context, a detailed case study of the Prevention of Electronic Crimes Act (PECA) 2016 in Pakistan highlights the tensions between comprehensive criminalization and civil liberties protection, including documented overblocking of online content. Four dimensions of enforcement challenges are considered systematically: jurisdictional ambiguity, difficulty of attribution, lack of forensic capacity and low reporting rates. Finally, the article emphasizes the importance of not only having coherent legal frameworks in place, but also of continuous investment in institutional capacity, in PPs, and in the need for a balanced security approach and respect for fundamental rights.*

Keywords: Cybercrime legislation, Budapest Convention, Prevention of Electronic Crimes Act, digital forensics, jurisdiction, online censorship, public-private partnership

Introduction

The internet has radically changed the way people communicate, do business and organize their communities in the twenty first century. For example, in 2000, only 361 million people (about 6 per cent of the world's population) had access to the World Wide Web (Hawdon, 2021). By 2024, that number had grown to almost 5.4 billion users, including over 2/3 of the world's population. The digital revolution has brought tremendous economic and social advantages: it allows for instant global communication, the sharing of information is levelled and made accessible to everyone, and it has given birth to new industries. But as Brenner (2012) has noted, the very advantages of the Internet, its speed, anonymity, ubiquity, and low transaction costs are also its great disadvantages for criminals.

Cybercrime is the type of crime that defines the current century, kind of like larceny in the 1900's, and highway robbery in the 1700's.Cybercrime is the crime of the century, just like larceny in the 20's and highway robbery in the 17's. Cyber crimes do not necessarily involve the need for the offender to be in close proximity to the victim or necessarily involve a quantifiable amount of stolen property, but rather can occur from anywhere in the world with an Internet connection, can inflict harm on millions of people at once, and can result in devastating systemic consequences with little or no physical investment on the part of the perpetrator. The economic consequences are enormous. According to cybersecurity analysts, the global impact of cybercrime in terms of lost productivity, ransomware payments, system restoration and data breaches is projected to total $10.5 trillion annually by 2025 (Wall, 2024). When taken as a whole, this is more than the gross domestic product of all but the top two world economies, making cybercrime the third largest economy in the world if considered separately.

The growing reliance of societies on digital technology, which is used for critical functions like financial services, energy grids, transportation systems, healthcare delivery and governmental operations, has made it more important than ever to have strong legal and enforcement frameworks in place. However, the creation of effective legislation against cybercrime has not followed the technological advances of crime methods by any means (Babanina, Tkachenko, Matiushenko, & Krutevych, 2021). It's a tough dilemma for lawmakers. First, they have to devise legislation that punishes acts that could never have been imagined when it was written and which must be either very expansive and flexible or constantly amended. Second, they need to create enforcement mechanisms that are inter-jurisdictional, but do not violate basic rights, including privacy, freedom of expression and due process.

This article performs an analytical study of the laws and policing of cybercrime in the twenty first century in a systematic manner. The analysis is carried out in five steps. Part I further clarifies the definitional scope of cybercrime, breaks down the various types of offenses and highlights the particular characteristics of cyberspace which present challenges for legal action. Part II explores the international legal environment, such as the Budapest Convention, regional alternatives and the emerging UN convention. The national case study in Part III showcases the prevention of electronic crimes act, 2016 in Pakistan and the challenges of its implementation. Part IV explores ongoing enforcement issues that have hindered even the most innovative legal instruments such as jurisdictional uncertainty, attribution difficulties, forensic capacity deficits and low reporting rates. Part V deals with the basic conflict between security measures and civil liberties, and examines the European methods of data protection against documented over-regulation in Pakistan. The results are summarized and a comprehensive solution plan for cybercrime governance is suggested in the conclusion.

Part I: Defining the Digital Threat: A Refined Typology of Cybercrime

An accurate mapping of cybercrime is essential to developing sound legislation and enforcement. The term, however, has proven to be difficult to define because it refers to a diverse range of crimes with varying technical structures, legal requirements, victim populations and degrees of difficulty in prosecution.

1.1 The Three Category Typology

There are three general types of cybercrimes, according to the scholarly typology, which is based on the relationship between the cybercrime and the computer system (Finklea & Theohary, 2012). Firstly, cybercrime against the machine is the attacks on integrity, availability or confidentiality of computer systems and networks. These include unauthorized access (hacking), introduction of malicious code (viruses, worms, ransomware), a distributed denial of service (DDoS) attack, where servers are overwhelmed in traffic and sabotage of critical infrastructure. These crimes are crimes directly committed to the computer system. Second, cybercrimes committed with the machine are transpositions of traditional crimes, so that the computer is a tool or instrumentality. Some of the most popular include online fraud, identity theft, phishing attacks, credit card cloning, and ransomware or sextortion. The

criminal conduct itself – deception or coercion – is not new; the medium through which it is being done is new. Third, machine related offences are those offences where the computer system is used to store or distribute illegal content. This encompasses the sharing of child sexual abuse material, hate speech, terrorist propaganda and revenge pornography. The offense involves the creation or possession or transmission of content that is prohibited, even if it is not possible to prove that any particular victim is harmed (Finklea & Theohary 2012).

This typology of three categories is analytically useful as it aligns with various legal treatment and enforcement strategies. Offences committed against the machine usually involve computer misuse or data protection laws and would be dealt with by a technical forensic expert. The offenses committed with the use of the machine are frequently treated in general criminal statutes, but the application of conventional evidence rules to digital environments is complicated. Mischief committed by the machine presents complicated challenges about free speech and content regulation, which overlap with constitutional protection issues (Wall, 2024).

1.2 Unique Features of Cyberspace That Complicate Legal Responses

Cybercrime is not simply "old crime gone new," but has unique characteristics that change the equation of crime and law enforcement. Brenner (2012) recognized a number of such features. First, in cyberspace, geographical boundaries do not exist. One bad guy sitting at a cybercafe in Karachi can penetrate a financial institution in New York, encrypt the servers with ransom and ask the institution to pay up in cryptocurrency in a dozen countries. All of these happen in milliseconds and evidence bits are spread across jurisdictions. There is no territorial barrier to cross and the traditional territorial jurisdiction principles are hard to apply or are not applicable at all.

Secondly, the internet promotes anonymity, which systematically reduces the chances of detection and identification. A virtual private network (VPN), the Tor anonymity network, a compromised third party computer (botnets), or a hotspot for public WiFi may serve as a route for communication for an offender. They have the ability to transact using cryptocurrencies that conceal the trail of transactions. They can use encrypted messaging apps that law enforcement can't access, disposable email addresses and false identities (Brenner, 2012). One of the core characteristics of cybercrime is the asymmetry between those who are perpetrators and those who are victims. A victim recognises that a crime has been committed, typically as a result of a monetary loss, or a disruption to the system, but is unable to identify the perpetrator. Unlike traditional crime, in the traditional case the victim and offender are usually physically present at the same time and can be easily identified or described.

Thirdly, cyber operations are conducted at a speed and scale that causes enforcement latency. A standard burglary could involve just one residence and only last for a few minutes to hours. A DDoS attack can impact thousands of websites and incur millions of dollars of losses in just a few seconds. By contrast, police work moves at the pace of humans, and calls for subpoenas, forensic analysis and mutual legal assistance requests that take weeks or months. When the time comes for an offender to be identified, the offender has already committed hundreds of other offences (Broadhurst, 2006). Fourth, the low cost of entry and high scalability of cybercrime reduces traditional barriers to offending. Exploit kits, ransomware-as-a-service and stolen credit card databases can be bought on a dark web marketplace for as little as a few hundred dollars, a person with moderate technical skills can purchase them. It's the same tools used against one victim that are used against one million victims with little extra work. This facilitates a criminal economy where even those with limited capabilities can make a lot of money, as opposed to traditional property crime, which requires physical presence, skill and risk of apprehension (Wall, 2024).

These attributes have been the subject of some commentators to compare cyberspace to an ungoverned, lawless Wild West (Rho, 2007), which is aptly apt due to the lack of effective territorial sovereignty, the speed of the conflict and the challenges of establishing order. But as this article will show, the Wild

West metaphor doesn't fit completely. Cyberspace is, of course, different from the American frontier of the past, where federal laws eventually spread into the area, but which has no such mechanism of institutionalizing authority. There is no international cyber police force. There is no universal cyber jurisdiction in the world court. Even the strongest of national governments have trouble controlling activity emanating from outside their countries and passing through governments that are either unwilling or incapable of cooperating (Fidler, 2025).

Part II: International Legislative Frameworks – Harmonisation, Fragmentation and New Alternatives

Cybercrime is inherently a transnational phenomenon, making a case for international cooperation and legal harmonization. No single national legal system is able to deal with criminal acts that originate in a country, move through servers in another and are transacted in the third, and that are harmful to that country. However, history shows a long-standing gulf between the goal of convergence and the fact of political division in international cybercrime law.

2.1 The Budapest Convention on Cybercrime (2001)

The Convention of the Council of Europe on Cybercrime opened for signature in November 2001 in Budapest is the most important multilateral agreement in the field. It marked the first international agreement ever to be formulated specifically for the development of a common criminal policy for cybercrime and it has been used as a template for legislation in over 60 countries, comprising many non-European states (Fidler, 2025). The Convention is divided in four substantive chapters. Parties shall define under their domestic law criminal offenses concerning illegal access, illegal interception, data interference, system interference, misuse of devices, computer related forgery, computer related fraud, child pornography offenses and copyright infringement. Chapter III sets out the procedural powers that need to be put at the disposal of the law enforcement authorities, such as the ability to produce orders for the preservation of information held on the network, orders for the production of information on subscribers, search and seizure of computer systems, and collection of traffic data in real time. Chapter IV brings together the framework for international cooperation, such as mutual legal assistance, extradition and a network of contact points available 24 hours a day for urgent requests. Final clauses concerning signature, ratification and reservations (Fidler, 2025) are included in Chapter V.

The Budapest Convention is a highly praised and criticized convention. Proponents say that it serves as a much needed minimum level of criminalization, allows for cross border evidence collection, and has led to dozens of countries having cybercrime legislation which previously did not exist (Broadhurst, 2006). Some critics, especially from developing nations and authoritarian states, contend that the Convention was written by rich western countries with minimal input from the global south, that the process of its drafting did not include robust safeguards for procedural evidence collection and that it does not include any consideration of the use by state actors of cyber tools for espionage or political repression (Fidler, 2025). These objections have become more pronounced as more non-European nations have joined the Convention, including the Japanese, Canadian, Australian and American, with many major developing countries, including Brazil, India, Indonesia and Pakistan, not participating.

2.2 Regional and National Balancing and Regional Cooperation

As a result, there are regional alternatives to the Budapest Convention that embody alternative geopolitical approaches and conflicting understandings of digital sovereignty (Fidler, 2025). The Shanghai Cooperation Organization (SCO), comprised of China, Russia, and some Central Asian countries, has pushed for a model based on greater state oversight of the internet, criminalisation of content deemed to endanger national security or social stability, and mutual legal assistance confined to member states. The Arab Convention on Combating Information Technology Offenses, adopted by the League of Arab States in 2010, also focuses on state security interests, and contains wide definitions of prohibited information. In 2014, the African Union adopted the Convention on Cyber Security and

Personal Data Protection, which incorporates cybercrime and data protection and electronic commerce provisions, but has been not quickly ratified (Fidler, 2025).

This disagreement is not just a drafting disagreement. It speaks to the issue of how the state should be involved in the regulation of online speech, and the scope of law enforcement access to encrypted communications, and the authority to gain access to cross-border evidence without the consent of the host state. However, the model supported by western democracies – principally the European Union and the United States – tends to criminalize a core set of offenses, affords strong procedural protections for suspects, and enables fast mutual legal assistance. Authoritarian states and most developing states prefer a model where states have wide discretion in determining what is prohibited, few limits on investigative powers, and cooperation is contingent on political compatibility (Fidler, 2025). Such differing preferences have hampered the development of a truly global cybercrime treaty, and created a mix of overlapping and conflicting obligations.

2.3 The United Nations Convention on the Elimination of All Forms of Discrimination against Women in the Field of Science

To address this disintegration, the United Nations (UN) General Assembly began working on a new global convention on cybercrime in 2019, which became the United Nations Convention on Cybercrime in 2024 (Fidler, 2025). In an attempt to overcome the differences between the Budapest model and the regional alternatives, the UN Convention takes a hybrid approach. It contains the core criminalization elements found in the Budapest Convention like illegal access, computer related fraud or data interference. It also contains provisions on content based offences such as child sexual abuse material and importantly, racist and xenophobic propaganda, a topic which was long favoured by developing countries and some western free speech advocates and opposed by others. The Convention introduces a new system of mutual legal assistance, which includes provisions for direct cooperation without the use of the diplomatic channels in urgent cases, and also guarantees the protection of human rights and data protection. It also contains a specific obligation to abide by existing international human rights commitments in the implementation of cybercrime legislation (Fidler, 2025).

The UN Convention is not without its critics. Critics from civil society groups have raised the fear that its definition of racist and xenophobic propaganda could be used to quell any political opposition. Digital rights groups have pointed out that the Convention contains no judicial authorisation requirements for the production orders or data retention measures that are part of the European Union data protection framework. By contrast, law enforcement has contended that the Convention does not provide enough obligations to the service provider to ensure that it responds to requests from foreign authorities, thus leaving the same jurisdictional gaps that have long bedeviled enforcement since the 1940s (Fidler, 2025). Despite these complaints, the UN Convention is the largest and most important step forward in cybercrime law in the international arena since Budapest. If ratified by a sufficient number of states, it could begin to harmonize the fragmented landscape, though its effectiveness will ultimately depend on the willingness of parties to comply with its obligations and to resolve disputes through the mechanisms it establishes.

Part III: National Legislation in Practice: The Case of Pakistan's Prevention of Electronic Crimes Act 2016

It is useful to look at a particular national case to understand how international frameworks are interpreted in the domestic sphere and applied. To this end, Pakistan is illustrative of a large developing nation with rapid growth of Internet usage, high rates of cybercrime victimisation, and high and growing domestic and international levels of engagement with the legislative response.

3.1 Legislative History and Rationale

The Pakistani cybercrime laws prior to 2016 were incomplete and scattered.Pre-2016 the laws of

cybercrime in Pakistan were known to be inadequate and disjointed. Some provisions of the general Pakistan Penal Code 1860 were applicable to certain digital crimes like fraud or forgery, but they were framed in the 19th century and were not specific to computer systems like unauthorized access, data interference etc. The Electronic Transactions Ordinance 2002 provided some legal recognition for digital signatures and electronic records but created no criminal offenses. The Investigation for Fair Trial Act 2013 sought to address some of the procedural problems that may arise in the collection of electronic evidence, but failed to criminalize any substantive offences. This posed major challenges for the investigation and prosecution of cybercrime by law enforcement, and there was little recourse for victims (Akhlaq, 2021).

In 2015 the government of Pakistan presented the Prevention of Electronic Crimes Bill and it became Prevention of Electronic Crimes Act (PECA) 2016 after much debate in parliament and its assent by the president of Pakistan. The goals of the Act were to fight against unauthorized acts concerning information systems, investigate electronic crimes, prosecution of electronic crimes and cooperation at the international level in cybercrime issues (Idrees, Hussain, & Shahid, 2016). The Act was clearly based on the Budapest Convention, which Pakistan has not ratified. It was an amalgamation and expansion of cybercrime provisions into one single dedicated law, making Pakistan a part of the legislative framework of its neighboring countries such as India, Bangladesh and other countries in the region.

3.2 Substantive Offenses Under PECA 2016

PECA 216 contains 21 substantive offence sections which criminalise a vast array of behaviour. The following are some of the most important. Accessing an information system without authorization is punishable under section 4 with imprisonment of up to three years, and fines of up to one million Pakistani rupees. Authorized copying or transmission of data is considered a crime in Section 5 with like penalties. Section 6 of the bill makes electronic forgery punishable by up to seven years imprisonment (criminal acts involving the creation or modification of electronic data with intent to cause harm or fraud). Part 7 criminalizes electronic fraud, punishable by up to seven years imprisonment and fines. Section 8 makes it illegal to use personal identifying information without authorization (identity theft) punishable by up to three years imprisonment. Section 9 is directed against fraudulent issuance of electronic payment instruments, which is a term that encompasses credit and digital payment fraud. Section 10 makes it a criminal offense to use electronic communications to harass, intimidate or threaten a person, with penalties of up to three years imprisonment. Section 11 criminalizes the production, possession and distribution of child sexual abuse material, carrying a level of severity of up to seven years imprisonment and fines. Section 14 and 15 criminalize cyber terrorism with a prison term of up to 14 years or life imprisonment if the purpose of such access or interference is to cause death, injury or damage to any critical infrastructure (Akhlaq, 2021; Iqbal et al., 2023).

The Act also provides for the procedure allowing the Federal Investigation Agency (FIA) to investigate offenses, enter, search and seise electronic devices and obtain subscribers information from internet service providers. The FIA has been established with a special Cyber Crime Investigation Wing in Section 34. The federal government has the power to instruct service providers to prevent access to material that is deemed to be unlawful under the Act, even without court permission in emergency situations (Kamran, Arafeen, & Shaikh, 2019).

3.3 Implementation, Enforcement Gaps, and Civil Society Criticism

Although the legislative intent of PECA 2016 is ambitious, there have been numerous problems implementing the legislation. The problem with FIA's Cyber Crime Wing is that it is understaffed, there is a lack of digital forensics training and the backlog of cases has been a long-time problem. By 2021, there were more than 100,000 complaints received by the Wing, but investigations were only completed in part of these complaints, and prosecutions were even lower (Iqbal et al., 2023). There are numerous

anecdotal examples of complainants dropping their cases because it takes too long for investigations and because of the difficulty of the complainant in providing admissible electronic evidence.

More importantly, PECA 2016 has received heavy criticism from civil society groups, news agencies and human rights groups. Critics say that the Act is draconian and allows too much discretion for the executive powers to limit online speech (Khan & Anwar, 2020). The main concerns can be divided into three areas. First, the definition of offenses like cyber stalking and cyber terrorism is overly broad, that could include legitimate political speech or journalistic reporting. Second, the blocking provision in Section 37 is poorly supervised, as the government can take content down without being able to show it violates any constitutional requirement of harm. Third, the punishments are too harsh, with the penalties of some of the offenses being more severe than those associated with similar physical offenses (Idrees et al., 2016; Akhtar, 2023).

Some of these concerns are substantiated by empirical evidence. Digital rights organisations estimate that some 900,000 websites have been blocked in Pakistan since 2016 through the action of PECA and other laws. The reasons given for blocking were imprecise (e.g., 'against the glory of Islam' or 'against public order') and there was a lack of public information about what was being blocked and why it was being blocked (Khan & Anwar, 2020). This chilling effect applies to journalists, activists as well as ordinary citizens, who may be inclined to self censor due to a fear that protected speech could be considered illegal under the broad scope of the Act. A comparative study by Ahmad and Akhter (2026) found that Pakistan's cybercrime framework, while similar in structure to the United Kingdom's, provides significantly fewer procedural safeguards for suspects and targets, and gives the executive broader authority to restrict content without judicial review.

3.4 Comparative Performance: Pakistan Versus Regional Neighbors

A short comparison is included to give perspective to Pakistan's experience. The Information Technology Act, 2000 (substantially amended in 2008), also criminalizes such acts of unauthorized access, theft of information and cyber terrorism in India. Some of the provisions in the Indian Act are also criticized as being too broad, especially Section 66A which criminalized offensive messages, due to its violation of free speech and struck down by the Supreme Court in 2012. India has, however, taken greater efforts to strengthen the forensic infrastructure, in the form of the Indian Computer Emergency Response Team (CERT In) and regional cybercrime coordination centers, and has resulted in better prosecution rates for some crimes (Ahmad & Akhter, 2026). Following the Digital Security Act (DSA), Bangladesh enacted in 2018, which has been even more harshly condemned than PECA for its broad interpretation of defamation as well as its harsh punishments. In several instances international observers have recorded journalists and opposition politicians being jailed for writing articles critical of the government, all of which were done under the Act. The PECA 2016 comes amid the continuum between Bangladesh's Digital Security Act and Pakistan's less restrictive, but more substantially and less procedurally protective, amended IT Act (Ahmad & Akhter, 2026).

Part IV: Enforcement Challenges: From Jurisdiction to Digital Forensics

Well drafted legislation to combat cybercrime is only of limited value if the law enforcement agencies are unable to investigate crime, identify perpetrators and obtain convictions. In the world today, law enforcement officials are hard pressed to catch up with cyber-criminals who are adept at wielding technology and evading detection, and large gaps make even the best legislation ineffective.

4.1 Jurisdictional Ambiguity and the Territoriality Problem

The power of a state to make law, settle disagreements, and carry out decisions within its own area. Traditional criminal jurisdiction is based on territory, that is, a State can prosecute crimes that occur within its borders. Cybercrime, however, is frequently trans-border in nature, as the perpetrator, the victim, the computer servers and the impact of the crime can be situated in disparate countries (Brenner,

2012). Assuming a hacker gains access to a German server for example, and steals data from a cloud provider's server in Ireland, and then uses that data to defraud a victim in Australia, in which country does the crime take place? All of them could assert their jurisdiction under different principles: territoriality (place of the occurrence of an act, place of the victim's effect of the act), nationality (place of the offender, place of the victim), passive personality (place of the victim), universality (for some grave crimes). This can lead to parallel investigations, competing extradition demands, or most frequently to no investigation whatsoever as each state assumes that another will investigate (Broadhurst, 2006).

The Budapest and UN Conventions are trying to settle any jurisdictional disputes in a hierarchical way. The first is based on territoriality, which is the jurisdiction of the state in which the offense was committed. If there are more than one states with territorial claims, they are expected to coordinate with each other, and a state where the offender is likely to be in the forefront. But in practice, there is very little coordination, especially if the offender is in a country without extradition treaties with the victim's country or unwilling to prosecute its own nationals (Fidler, 2025). The outcome is that many transnational cybercrimes go unpunished.

4.2 Attribution: The Technical and Evidentiary Challenge

When there is jurisdiction, it is necessary for law enforcement to determine who committed the offence. Attribution is the identification of the source or originator of a cyber act that is observed. With the traditional crime, it is often easy to establish who committed the crime, thanks to eyewitnesses, prints, DNA, and confessions or alibis. In the cybercrime world, it is a challenge to determine who is behind an attack (Brenner, 2012). The criminals are employing multi-layered anonymization methods such as VPNs, the Tor network, public WiFi and tainted third party machines. They employ cryptocurrency mixers which make it harder to trace the transaction flow. They incinerate or scramble evidence themselves. Even if a forensic investigation can identify the IP address of an attack, the address can belong to an innocent third party whose computer was hacked and used as a "relay" or it can be a WiFi hotspot in a coffee shop where the person who committed the attack was physically present for only a few minutes, and left no identifying marks.

The attribution problem is especially complex with regard to state-sponsored cyber operations because the perpetrator could be a paid intelligence agent who is operating within the remit of a state directive. Technical attribution can determine the country state of origin of a specific attack, through code reuse, command and control infrastructure or operational patterns. However, it's much harder to translate technical evidence into evidence that would be acceptable in a criminal case and meet the standard of proof. Offenders employ false flags, on purpose mimicking the methods of other states to fool attribution. They use the system of cut outs and proxies to disrupt the chain of evidence. Because of this, most nation state cyber operations are dealt with diplomatically or economically, and not criminally (Wall, 2024).

4.3 Forensic Capacity and the Skills Gap

Digital forensics is the use of science to preserve, retrieve and analyze electronic evidence in support of a legal action. Digital forensics techniques are very technical and require special expertise to image a storage medium in a forensically sound manner, to recover deleted files, to parse log files and metadata, to decrypt encrypted files within legal limits, and to present complex technical details in a manner that is accessible to judges and juries. Many police services, especially in developing countries, do not have these capabilities (Broadhurst, 2006). According to the 2023 study carried out by the FIA Cyber Crime Wing, only 20 per cent investigators were trained in digital forensics, and the equipment available in the forensic labs was outdated and unavailable while there is no recognized digital forensics certification program in Pakistan (Iqbal et al., 2023). The lack of capacity is not unique to the United States, and is also present in other jurisdictions, such as some of the European countries that have lower

budgets for law enforcement technology.

Rapid technological change is enhancing the skills gap. Law enforcement is always one step behind in being able to keep pace with the evolution of various encryption algorithms, storage media, and new obfuscation techniques. There are months or years of training in traditional police training cycles to prepare them for a field in which the technologies involved evolve every 18 to 24 months. Others have taken steps to establish cybercrime units, expedite training programs, and forge partnerships with cybersecurity industry companies to address the issue. Others have assigned forensic analysis to private contractors, where they have questioned the chain of custody and data privacy (Broadhurst, 2006).

4.4 The Dark Figure of Cybercrime: Latency, Underreporting, and Victimization Surveys

The dark figure of crime is a well-recognized fact by criminologists that official crime statistics only reflect a fraction of the total amount of crime. The dark figure for cybercrime is believed to be very high for cybercrime, at 85-90 percent (Hawdon, 2021). There are multiple reasons why the underreporting occurs. Data breaches or unauthorized access without any obvious signs may lead to many victims not being aware that they have been victimed. Other victims are aware of the harm that was done to them but fail to report it for one or more of the following reasons: the police do not seem to have the ability to investigate; they may be embarrassed or suffer reputational damage if they do report it; they may think that the damage done is not worth reporting. Vitamins and minerals may not be corporate victims, as there might be positive incentives for them not to disclose, especially if it would lead to repercussions such as regulatory fines, shareholder lawsuits, or damage to customer trust (Wall, 2024).

Latency is another term that is used in relation to time that lapses between the commission of an offense and its discovery. For many cybercrimes, latency is in months or years. A data breach can be discovered in December when a routine audit is conducted, even though it happened in January.It could happen in January and only be discovered during December when a routine audit was conducted. The time it takes to discover the breach may have allowed time for forensic evidence to become compromised, logs to be overwritten, and the attacker to be on to the next target. This delay not only reduces the deterrent value of the criminal law – the criminals know that they will likely be undetected and that the crime will be delayed – but also the remedial value – victims are exposed to more hurt than necessary due to the delay (Hawdon, 2021).

A more accurate picture is given by victimisation surveys, which ask representative samples of the population about their experiences of cybercrime, whether or not they were reported to the authorities. A series of cross national surveys by the United Nations Office on Drugs and Crime (UNODC) and academic researchers have shown that the incidence of cybercrime victimization is significantly greater than the rate of police-reported victimisation. For instance, the number of people who are victims of some type of online fraud, identity theft or unauthorized access on the Internet is 10-20% of internet users over the past year, but only 5% of these who are victimized report the crime to the police. This disparity is even greater for types of victimization like cyberstalking or cyber harassment, where victims might think that the offense occurred or that they would face retaliation if they reported it, or that it wouldn't be taken seriously by authorities (Hawdon, 2021).

4.5 Public Private Partnerships as a Partial Remedy

Many experts are urging for public-private cooperation that will take advantage of the expertise and resources of the private sector because of the limitations of public law enforcement. Most law enforcement agencies lack the threat intelligence, forensic tools and real time monitoring data that internet service providers, cloud hosting providers, financial institutions and cyber security companies have. They also have direct contractual agreements with victims and are able to take remedial action, such as blocking malicious traffic, freezing fraudulent accounts, etc., without engaging in any legal process (Broadhurst, 2006).

Public Private Partnerships can be done in many different ways. Information sharing agreements enable companies to pass on information about cyber threats and attack patterns to law enforcement without incurring any risk of antitrust or data protection violations. Private sector analysts are integrated into police cybercrime teams in the form of joint task forces. The public forensic laboratories or training academies can be funded by funds from the private sector as well. Partnerships, on the other hand, have their own set of concerns, though. Private companies are not subject to the same constitutional and statutory limitations as public law enforcement agencies, and the delegation of investigative powers to private companies can avoid due process limitations. Other conflicts of interest exist: A business's first obligation is to their shareholders, not the public interest in law enforcement or the provision of information which may be used against the company to bring about regulatory action (Broadhurst, 2006). Even with these considerations, the literature is largely unanimous that public private partnerships are not only useful but essential in combating cybercrime, especially in its size and complexity.

Part V: Balancing Security and Civil Liberties: The Central Dilemma of Cybercrime Legislation

One of the greatest challenges for twenty first century cybercrime legislation is balancing citizens' rights to protection from digital threats with the rights to fundamental freedoms of speech, privacy, and due process. This section explores how various jurisdictions have dealt with this tension and lessons learned from the successes and struggles.

5.1 The European Model: The General Data Protection Regulation as a Framework

General Data Protection Regulation (GDPR), which entered into force in 2018 in the European Union, is not a cybercrime law, but a law pertaining to data protection and privacy. It has been a central element in the European cyber governance landscape, however, because it sets strong rules for how personal data is collected, processed and kept by both the public and the private sector (Krüger, 2026). The GDPR requires that access to personal data by law enforcement be based on a specific legal basis, limited to what is necessary for the specific task, notify individuals of any data breaches, and afford individuals rights of access, rectification and erasure. The GDPR also has a requirement for businesses to have appropriate security measures in place and also notify of data breaches within 72 hours.

In the context of cybercrime, the GDPR is trying to achieve two goals in opposition. It also gives law enforcement access to tools to investigate offenses, such as measures that enable member states to put in place data retention obligations for security reasons and to authorise access to electronic evidence with judicial oversight. Then again, it sets limits to guard against unwanted surveillance and data use by people. For instance, the Court of Justice of the European Union has consistently ruled that the GDPR and the EU Charter of Fundamental Rights do not allow for the retention of data in a general and indiscriminate manner, prompting the need for targeted data retention, the limitation of the retention period and the independent authorisation of the retention. (Krüger, 2026).

Critics of the European model claim GDPR's safeguards are excessive, which would make it difficult for police departments to conduct effective investigations of cybercrime, especially when evidence is kept in various countries with different regulations. As for the rest of the world, supporters state that the GDPR offers a template for the rest of the world, indicating that robust data protection and effective cybercrime enforcement do not need to be incompatible, but instead reinforcing each other, as public trust in the digital systems that are the foundation of the internet depends on both its security and data privacy (Krüger, 2026). The evidence is mixed, but some studies have identified no clear connection between strong data protection laws and rates of cybercrime clearance, meaning that other factors, including forensic and capability and international cooperation, play a greater role.

5.2 The Pakistani Experience: Overblocking and the Chilling Effect

There has been criticism that the Pakistan's PECA 2016 has taken the debate too far and prioritised

security and government over civil liberties, as discussed in Part III. The blocking provision in Section 37 causes major concerns, as it allows the government to require ISPs to block access to online content without any judicial oversight, bearing in mind that it is up to the government to decide whether the content is illegal under the Act. The Act does not allow for judicial review after the blocking, a victim to find out that his/her content is blocked, or to have a voice in challenging the blocking order, or even to find that his/her content is already removed from the platform and cannot be restored (Khan & Anwar, 2020).

About 900,000 webpages were blocked in the period 2016-2019 according to PECA and related laws, indicating that the government has taken a broad approach to its powers. Many of the blocked pages featured political speech against the government, information on a particular topic that was sensitive, such as military operations or judicial corruption, or information that was considered blasphemous by Pakistan's blasphemy laws. Civil society groups have reported instances of whole news sites being blocked for days or even weeks, based on one article they were ultimately found to be lawful (Idrees et al., 2016). The chilling effect is not hypothetical, it's real and measurable. According to survey results published in 2020 and 2023, over 60 percent of journalists in Pakistan said they are self-censoring on certain sensitive issues for fear of legal action or blocking of websites under PECA and nearly 40 percent had personally faced or observed the blocking of journalists' content (Khan & Anwar, 2020).

The Pakistani experience is a warning to other developing nations which are in the process of enacting their own cybercrime legislation. Such vague and broadly drawn allegations and limited procedural protections are not just a drafting mistake; they produce predictable over-enforcement and under-enforcement of the law against disfavored speakers and actual cybercriminals, respectively. The budget allocated to prevent political speech could be used instead to investigate online crimes such as online fraud, online identity theft, and child exploitation that impact real victims, and the crimes that the public desires police attention to be directed toward (Ahmad & Akhter, 2026).

5.3 Toward a Principled Balance: Lessons for Legislative Design

What would a well-designed cybercrime law be like? Based on comparative literature and human rights principles, several design principles emerge (Christou, 2018; Graham, 2019). Offenses should be clearly and narrowly drawn to provide fair warning of prohibited conduct as well as to prevent giving too much interpretive discretion to the prosecutors and regulators. Words like against public order, indecent, harmful should be avoided and any restrictions on the basis of content must be narrowly drawn to meet an important public interest, for example, to protect children from sexual exploitation or incitement to immanent violence.

Second, that there shall be prior judicial authorization, unless in exigent circumstances, for all procedural powers such as search and seizure, production orders and real time surveillance, and that the judicial authorization shall include a showing of probable cause or reasonable suspicion of the person being searched. Collecting bulk data and general warrants without suspicion should be avoided.

Thirdly, blocking orders and requests for removal of content should be made via open, published and clearly explained processes and should always be accompanied by notice to the content provider and judicial review before it is removed, unless the content is so obviously unlawful that the notice would not serve the purpose of the removal, e.g. a platform such as child sexual abuse material refusing cooperation.

Fourth, penalties should be commensurate with the injury suffered, with more serious penalties for offenses that result in serious physical or financial damage, like cyberterrorism or massive fraud, and less severe penalties for offenses that result primarily in injuries to dignitary interests, or smaller damages. The harsh punishments for petty offenses, including a three-year prison term for the first offense of cyber stalking, if it involved no physical threat, are likely to be disproportionately imposed on marginalized populations and to burden courts with minor cases.

Fifth, mechanisms of independent oversight can help to curb executive overreach and remedy the violation of individual rights, such as a parliamentary commissioner for digital rights or an established tribunal for appeals of content removal. This is especially significant in countries where the judicial system is not independent or where the general population is unable to use ordinary courts (Christou, 2018).

Conclusion

Cybercrime is not a fleeting incident or a limited field of criminal justice, it is an industrialized, developing and structurally integrated part of the twenty first century information environment. This article has shown that the legislative and enforcement measures against cybercrime have not been able to catch up with the technological and social changes that create cybercrime. International frameworks don't have a uniform or universal approach, with the Budapest Convention as a model for some countries, regional approaches for others, and a new United Nations Convention making an effort to bring these two together. Though such laws may criminalize the right offenses, like PECA 2016 in Pakistan, they are insufficiently equipped with procedural protections resulting in excessive and disproportionate enforcement of protected speech and insufficient enforcement of actual cybercriminals.

Enforcement is tough. Jurisdictional uncertainty, challenges with attribution, lack of forensic skills, and underreporting add up to a dark figure of cybercrime that could be more than 85 percent of all crimes. No one reform, whether it is a new treaty, a new forensic laboratory, or a new public private partnership will fix all these issues. Instead, a comprehensive, multi level approach to cybercrime governance is needed, along with the following: harmonised international legal frameworks that establish clear jurisdictional rules and facilitate mutual legal assistance; law enforcement agencies sufficiently resourced and trained with specialised cybercrime units and forensic skills; and, strong public private partnerships, which enable access to the private sector's threat intelligence, while also respecting fundamental human rights, such as freedom of expression, privacy and due process; most importantly, cybercrime legislation that respects fundamental human rights, including freedom of expression, privacy, and due process.

The most overlooked and most crucial is the last one. In a digital society, the state's ability to dig into, search for, seize, and block digital content will only be growing. Any power not regulated by clear laws, effective monitoring, and judicial approval is sure to be misused. The past century of the twenty-first century has already seen plenty of examples, ranging from Pakistan's blocking of 900,000 web pages to the social credit system in China, and Russia's cybercrime laws that are being used to silence political opponents. The purpose of cybercrime laws is not just to secure as much as possible: Making security at the expense of liberty is not security. The objective should be to create a safe digital space, where national interests and citizens' constitutional rights are safeguarded. That will take more than technical knowledge and legal expertise, it will take political resolve to uphold the ideals of liberal democracy and the rule of law.

References

Ahmad, M. I., & Akhter, R. (2026). Cyber governance in transition: Evaluating the effectiveness of cybercrime and cybersecurity frameworks in Pakistan and the United Kingdom. *Pakistan Journal of Law, Analysis and Wisdom*, 5(2), 75 89.

Akhtar, S. (2023). *Assessing the cybercrime legislation in Pakistan: A comparative study of European Union and Pakistani cybercrime laws* [Unpublished dissertation]. University of the Punjab.

Akhlaq, M. (2021). Cybercrime in Pakistan: A study of the law dealing with cybercrimes in Pakistan. *PCL Student Journal of Law*, 5(1), 31 66.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of

formation, current state and ways of counteraction. *Amazonia Investiga*, 10(38), 113 122. https://doi.org/10.34069/AI/2021.38.02.10

Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. University of Dayton School of Law.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408 433.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society*, 19(3), 355 371. https://doi.org/10.1080/23745118.2018.1430722

Fidler, M. (2025). Fragmentation of international cybercrime law. *Utah Law Review*, 2025(3), 737 802.

Finklea, K. M., & Theohary, C. A. (2012). *Cybercrime: Conceptual issues for Congress and U.S. law enforcement* (CRS Report No. R42547). Congressional Research Service.

Graham, A. O. (2019). *Cybercrime: Traditional problems and modern solutions* [Unpublished thesis]. University of Glasgow.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 46(6), 837 842. https://doi.org/10.1007/s12103-021-09652-7

Idrees, R. Q., Hussain, N., & Shahid, A. (2016). Cybercrime laws in Pakistan: A critical analysis of the Prevention of Electronic Crimes Act, 2016. *Journal for Current Sign*, 5(2), 2390 2405.

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://doi.org/10.58341/srj.v2i4.35

Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing cyber laws and their role in legal aspects of cybercrime in Pakistan. *The Society of Digital Information and Wireless Communications (SDIWC)*, 1 12.

Khan, U. P., & Anwar, M. W. (2020). Cybersecurity in Pakistan: Regulations, gaps and a way forward. *Cyberpolitik Journal*, 5(10), 205 218.

Krüger, M. (2026). Cybercrime and data protection laws: Balancing privacy and security in the digital age. *International and Comparative Corporate Law Journal*, 14(1), 88 112.

Rho, J. J. (2007). Blackbeards of the twenty first century: Holding cybercriminals liable under the Alien Tort Statute. *Chicago Journal of International Law*, 7(2), 695 728.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.