ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 01. July-September 2025.Page#.834-848
Print ISSN: 3006-2497 Online ISSN: 3006-2500
https://doi.org/10.55966/assaj.2025.4.1.064
Platform & Workflow by: Open Journal Systems

Unmasking Digital Deviance: Analyzing Cybercrime Trends via Social Media in Pakistan

Fatima Rida Suddle (Corresponding Author)
Lecturer, Department of Law, University of the Sialkot, Sialkot, Pakistan
suddlefatima@gmail.com
Samreen Pervaiz
LL. M. Scholar, University of the Punjab, Lahore, Pakistan
samreenpervaiz478@gmail.com
Sehar Nawaz
Lecturer, Department of Law, University of the Sialkot, Sialkot, Pakistan
seharwarraich15@gmail.com

ABSTRACT

The proliferation of social media in Pakistan has led to a significant rise in cybercrime, posing serious challenges to individuals, society, and legal systems. This paper examines the historical context and evolution of cybercrime, its conceptual foundations, and its manifestation on social media platforms in Pakistan. By analyzing the notion of crime through the perspectives of eminent jurists such as John Austin, Jeremy Bentham, and J.W. Cecil Turner, the study establishes the essential elements of criminal conduct and their applicability to the digital domain. The paper traces the origins of cybercrime from early telegraph manipulations in the 19th century to the sophisticated mobile-based threats of the contemporary era, highlighting the adaptive nature of cybercriminals and the vulnerabilities of emerging technologies. Focusing on the Pakistani context, the research identifies six major categories of social media-related cybercrimes: phishing and social engineering, hacking, malware dissemination, identity theft, spamming, and cyberbullying/harassment. The paper underscores the pressing need for comprehensive legal frameworks, enhanced digital literacy, and robust cybersecurity measures to combat the escalating threat of cybercrime. It advocates for a multi-stakeholder approach, encompassing legislative reform, institutional enforcement, public awareness, and private sector cooperation, to mitigate the harmful consequences of digital offenses and protect individuals' rights in cyberspace. The research contributes to the understanding of cybercrime's conceptual underpinnings, historical development, and contemporary manifestations, while emphasizing the urgency of effective countermeasures in Pakistan's rapidly evolving digital landscape.

Keywords: *Social Media, Internet, Cybercrime, Digital Deviance, Pakistan.*

1. Introduction

Social media has recently become an essential aspect of daily life, enabling individuals to exchange ideas and information while exercising their fundamental right to freedom of expression and speech. It represents a significant shift from traditional media in Pakistan, largely due to its growing prevalence. In Pakistan, social media is increasingly popular, especially among the youth (Hussain & Qureshi, 2018). The emergence of social media platforms has transformed, and will likely continue to influence, the ways in which individuals communicate and interact globally. Although the term “social media” lacks a precise definition (Hooker, 2019), it is commonly described in various dictionaries. Social media generally refers to internet- and technology-based tools that facilitate the sharing of information and dialogue (Tiwari & Ghosh, 2014). It provides a medium for communication through text, images, videos, and audio, combining elements of social interaction, telecommunications, and digital technology. Any internet- or digital-based platform that allows reciprocal communication between individuals and organisations, as well as the distribution of user-generated content, is considered "social media." The term commonly refers to specific platforms such as Twitter, Facebook, Snapchat, LinkedIn, and Instagram, often without recognising their unique attributes. It typically does not include platforms such as Wikipedia, Skype, and Netflix, nor does it encompass services that provide email or online news (Hooker, 2019).

In Pakistan, millions of individuals actively engage with a variety of modern social media platforms. As of early 2024, the country recorded 111.0 million internet users, reflecting an internet penetration rate of 45.7 percent. During the same period, the number of social media users stood at 71.70 million, constituting 29.5 percent of the total population. At the beginning of 2024, YouTube reported 71.71 million users in Pakistan, followed by TikTok with 54.38 million users, Facebook with 44.50 million, Snapchat with 30.21 million, Instagram with 17.30 million, LinkedIn with 12.00 million, and Twitter (X) with 4.50 million users (Kemp, 2024).

The widespread use of social media has given rise to significant challenges in Pakistan. It is increasingly employed as a tool for perpetrating various forms of technological, digital, and high-tech offenses. The collective term commonly used to describe these offenses is “cybercrimes.” Cybercrime is a broad term that encompasses all illegal activities carried out using computers, the internet, cyberspace, or the World Wide Web (Akhlaq, 2021). As defined by the official website of the Federal Investigation Agency (FIA), cybercrime refers to any act committed through computers, networks, and digital devices within cyberspace, facilitated by the internet. Such offenses include unauthorized access to remote systems for the purpose of stealing personal, governmental, or corporate data. Activities such as disseminating malicious software or publishing defamatory content on digital platforms also fall under the category of cybercrime (National Response Centre for Cyber Crime, n.d.).

The term "cybercrime" refers to a new type of illegal behavior that has evolved as result of the ongoing efforts of researchers to further scientific and technological advancements. The origin of the phrase "cybercrime" may be traced back to the English language, when the words "cyber" and "crime" were combined (Khalmuratov, 2024). The phrase is quite broad and encompasses a wide range of different types of criminal acts. Crimes committed online are closely related to those committed in traditional settings. Both include acts or omissions that violate the law and are susceptible to legal consequences imposed by the state (Goswami & Goswami, 2024). Both of these examples entail breaking the law. Generally speaking, there are two primary categories of cybercrime: those that directly target digital devices, such as hacking, phishing, spamming, identity theft, and denial of service attacks; and those that involve the use of technology to cause harm, such as cyberstalking, illegal gambling, blackmail, and online transactions related to the trafficking of people, drugs, gold, or weapons (Thakre, n.d.).

The misuse of social media has led to a notable rise in cybercrime. This issue demands urgent attention due to its potential to inflict harm on individuals and society at large. In 2018, more than

16,000 complaints were registered, which increased to over 48,000 in 2019. The number further escalated in 2020, with over 94,000 complaints recorded, and surpassed 100,000 in 2021 (Haider, Ali, & Zubair, 2023). A substantial portion of these complaints were filed under specific provisions of the Prevention of Electronic Crimes Act (PECA 2016), including Section 10 concerning Cyber Terrorism, Section 11 addressing Hate Speech, Section 20 related to offenses against the Dignity of a Natural Person, Section 21 involving crimes against the Modesty of a Minor and Natural Person, and Section 22 dealing with Child Pornography. Between January 1, 2021, and January 31, 2022, the Cyber Wing of the Federal Investigation Agency (FIA) resolved 100,986 complaints, while receiving 110,938 new ones. These statistics underscore the escalating nature of cybercrime and the pressing need for effective countermeasures.

In order to have a complete comprehension of cybercrime, it is first required to have a comprehensive understanding of the notion of crime.

2. Understanding the Notion of Crime

The term *crime* originates from the Latin word *crimen*, which historically signified an accusation or charge of wrongdoing. Over time, this term evolved to encompass acts that are not only morally reprehensible but also legally punishable. In modern legal discourse, crime is understood as a form of deviant behavior that violates established social norms and legal standards set by the state. Such conduct is considered harmful to the collective well-being of society and is, therefore, subject to formal sanctions under the law (Ajoy, 2024).

A crime is not merely a private wrong; rather, it is regarded as an offence against the public order or the state itself. It disrupts the legal and moral fabric of society and threatens the safety, security, and rights of individuals and institutions. As a result, the state assumes the responsibility to prosecute and penalize such acts through its criminal justice system. The classification and punishment of crimes vary depending on their nature and severity, but the unifying factor remains the breach of legal norms that are designed to maintain societal order and protect the public interest.

Definition of Crime

A number of eminent jurists and legal theorists have offered varying yet complementary definitions of the term *crime*, each reflecting their respective schools of thought and jurisprudential focus. These definitions contribute significantly to our understanding of crime within the broader context of criminal law and legal theory.

i. John Austin’s Perspective

John Austin, a renowned legal positivist, provides a distinct dichotomy between criminal wrongs and civil wrongs. According to Austin, a crime is a wrongful act or omission that is pursued by the sovereign or by state authorities in their official capacity. In contrast, if the pursuit of redress is initiated at the discretion of the injured party or their legal agents, the act is deemed a civil wrong rather than a criminal one. This classification places emphasis on who initiates the legal process, thereby distinguishing between private and public forms of legal injury. In Austin's framework, the involvement of state machinery in prosecution is a central characteristic of criminality (Goswami & Goswami, 2024).

ii. Jeremy Bentham’s Definition

Jeremy Bentham, a leading figure in utilitarian legal theory, offers a broader and more pragmatic definition. He asserts that a crime includes any act which the law forbids, whether such prohibition is based on sound reasoning or not. Bentham’s formulation is grounded in the principle of utility, suggesting that laws—justified or otherwise—serve to define what constitutes a criminal act. His approach recognizes that legal definitions of crime may not always align with moral or philosophical standards, but they are nevertheless binding as long as they are sanctioned by the law. Bentham's definition underscores the functional role of legislation in creating and maintaining the boundaries of criminal behavior (Goswami & Goswami, 2024).

iii. Glanville Williams' View

Glanville Williams, a leading British legal scholar, presents a more procedural and institutional definition. He defines a crime as an act or omission which amounts to a breach of law and for which criminal proceedings are prescribed, resulting in the imposition of criminal sanctions upon conviction. This definition emphasizes two key elements: legal breach and the application of criminal process, including prosecution, adjudication, and punishment. Williams' definition is notable for its focus on procedural consequences, rather than the nature of the act itself (Ajoy, 2024).

iv. Halsbury's Laws of England

In its third edition, *Halsbury's Laws of England* defines a crime as an unlawful act that causes harm to the public interest and renders the offender liable to punishment under criminal law. This definition highlights the public dimension of criminal conduct, asserting that crimes are not merely individual wrongs but offenses against the collective welfare of society. The inclusion of the term "unlawful act" reinforces the necessity of a legal prohibition, while the reference to public harm distinguishes criminal offenses from private disputes (Ajoy, 2024).

v. J.W. Cecil Turner's Analytical Framework

J.W. Cecil Turner offers a more structured and detailed account of crime by identifying three essential elements that characterize it:

a. **Harm caused by human agency**: Crime, according to Turner, originates from conduct or omission by a person that inflicts harm or poses a threat to societal interests.
b. **Prohibition by the state through punitive sanction**: Such conduct is of a kind that the sovereign authority seeks to prevent by declaring it punishable. The possibility of punishment acts as a deterrent against the repetition of such behavior.
c. **Determination of guilt through a formal legal process**: Turner also emphasizes the procedural aspect, where specialized legal mechanisms are employed to assess the culpability of the accused. If found guilty, the offender is subjected to punishment in accordance with the prescribed legal standards.

Turner's approach integrates both substantive and procedural aspects of criminal law. It offers a holistic view that accounts for the nature of the harm, the role of the state, and the requirement of due process in determining liability (Ajoy, 2024).

2.1 Essential Elements of Crime

Under the principles of common law, two fundamental elements must be satisfied for an act to constitute a criminal offence: the physical act (actus reus) and the guilty mind (mens rea). These components are encapsulated in the well-established Latin maxim:

Actus non facit reum nisi mens sit rea,

An act does not make a person guilty unless there is also a guilty mind.

This principle underscores that mere involvement in a prohibited act is insufficient to establish criminal liability unless it is accompanied by a culpable mental state. In other words, both the conduct and the intention or knowledge behind it must align to satisfy the legal threshold for criminal responsibility.

2.1.1 *Actus Reus* and *Mens Rea*

Actus reus refers to the external component of a criminal offence, encompassing conduct that is explicitly prohibited by law (Ajoy, 2024). It signifies the unlawful physical act or omission which forms the basis of criminal liability. Legal scholars have identified three essential components of *actus reus*: the prohibited act itself, the relevant surrounding circumstances, and the consequent result of the act. Importantly, the conduct must be voluntary; involuntary actions or reflexes do not typically satisfy the threshold of *actus reus*.

Conversely, *mens rea* denotes the guilty or culpable mental state of the accused at the time the *actus reus* is committed (Ajoy, 2024). It is considered the internal or subjective element of a crime and reflects the individual's intention, knowledge, recklessness, or negligence in relation to the unlawful act. As *mens rea* pertains to the mental processes of the offender, it remains inherently personal and is often not directly observable. Consequently, establishing *mens rea* through direct evidence poses significant challenges in judicial proceedings. Courts, therefore, frequently rely on inferences drawn from the facts and circumstances surrounding the offence to determine the presence or absence of the requisite mental element.

3. Understanding the Notion of Cybercrime

The concept of *cybercrime* is a relatively modern development that has evolved alongside advances in digital technology. Initially, the term *computer crime* emerged in the 1970s to describe unlawful activities involving computer systems. However, as technological innovation expanded the scope of digital devices and platforms, the terminology also evolved to reflect the changing landscape of criminal behavior. In this context, the term *cybercrime* was first introduced by Sussman and Heuston in 1995, marking a significant shift in the legal and academic discourse surrounding technology-related offences (Sabillon, Cavaller, Cano, & Serra-Ruiz, 2016)

While *cybercrime* has become widely used in legal, academic, and policy circles, there remains no universally accepted definition of the term. Originally, cybercrime was narrowly defined as criminal conduct executed through the use of computers (Saleem, Jan, & Areej, 2022). However, this early conceptualization has since been criticized for its limited scope, as it fails to account for the increasing role of other digital technologies, such as smartphones, tablets, and wireless networks, in facilitating cyber offences.

Modern understandings of cybercrime offer a more comprehensive and nuanced perspective. Cybercrime is now generally understood to refer to any illegal activity conducted through digital means, particularly via computer networks, the Internet, and mobile communication technologies. It includes actions directed against individuals with the intent to harm their reputation, mental well-being, physical safety, or financial interests, often carried out through digital channels such as email, social media platforms, online forums, and instant messaging services. Common examples include cyberstalking, online defamation, identity theft, cyberbullying, and the distribution of malicious software (Akhlaq, 2021).

A more extensive definition of cybercrime emphasizes both the criminal intent underlying such acts and the varied technological mediums through which they are carried out. This broader framing allows for a more accurate reflection of the dynamic and evolving nature of cyber offences. It recognizes that the digital ecosystem encompasses not only computers but also smartphones, wireless devices, cloud-based applications, and other interconnected systems that can be exploited for illicit purposes.

Hence, cybercrime should not be understood merely in terms of its technical execution, but also in light of its social, psychological, and legal consequences. It presents new challenges for legal systems around the world, particularly in terms of jurisdiction, evidence gathering, anonymity of offenders, and the rapid evolution of digital tools that facilitate such conduct.

3.1 Definition of Cybercrime

Over the past few decades, a number of definitions of *cybercrime* have been proposed by international bodies, legal scholars, and academic researchers. These definitions aim to conceptualize the evolving nature of crime within the digital realm. The term itself remains fluid and multifaceted, with no universally accepted definition to date—reflecting the complexity, diversity, and rapid technological advancement in the cyber domain. Below is an overview of six significant and widely cited definitions that attempt to capture the scope and essence of cybercrime:

i. 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000)

At the 10th UN Congress, two distinct definitions of cybercrime were introduced to accommodate both narrow and broad perspectives. In the narrow sense, cybercrime refers to “any illegal behavior directed at the security of computer systems and the data they process, store, or transmit,” involving the use of electronic means. This definition focuses on offenses that directly target information technology infrastructure, such as hacking or malware attacks.

In the broader sense, cybercrime is defined as “any illegal activity committed by means of or in relation to a computer system or network, including such crimes as illegal possession, offering, or distribution of information through a computer system or network.” This expanded view includes crimes that use computer systems as tools, not merely as targets, thus encompassing a wider range of activities such as fraud, data theft, and digital piracy (United Nations, 2000).

ii. Stanford Draft Convention (2001)

According to Article 1.1 of the Stanford Draft Convention on Cybercrime, the term is defined as “any crime involving cyber systems that is punishable under this convention.” This definition, while somewhat general, serves a functional and legalistic purpose, framing cybercrime within the parameters of a proposed international legal framework. It reflects an attempt to harmonize legal definitions for cross-border cooperation in cybercrime enforcement (Ajoy, 2024).

iii. Chris Hale (2002)

Chris Hale characterizes cybercrime as “activities conducted through computer systems and global electronic networks that are unauthorized or illegal according to certain jurisdictions or authorities.” This definition emphasizes the global nature of cybercrime, pointing out that actions considered illicit in one country may not be in another, thereby illustrating the legal complexities and jurisdictional inconsistencies in addressing cyber offenses across borders (Ajoy, 2024).

iv. Sarah Gordon and Richard Ford (2006)

Gordon and Ford offer a broader and more technological perspective, defining cybercrime as “any criminal activity that is facilitated or carried out through the use of computers, networks, or other hardware devices.” Their formulation acknowledges the instrumental role of technology in facilitating crimes, thereby extending the definition beyond conventional computer misuse to include crimes involving mobile devices, embedded systems, and other digital tools (Gordon & Ford, 2006).

v. Nir Kshetri (2009)

Nir Kshetri defines cybercrime as “high-tech crimes committed via computers or computer networks in violation of existing laws.” This definition aligns with the idea that cybercrime encompasses any unlawful conduct involving sophisticated technological tools, highlighting the growing complexity and technical proficiency required to investigate and prosecute such crimes (Ajoy, 2024).

vi. Samuel C. McQuade III (2009)

McQuade presents a practical and user-centric definition, stating that cybercrime involves “the use of internet-enabled devices such as mobile phones, computers, and personal digital assistants (PDAs) to engage in unlawful behavior and inflict harm.” His definition brings attention to the accessibility and pervasiveness of digital devices, acknowledging that cybercrime is not limited to sophisticated systems but can be perpetrated using everyday technology available to the general public (Ajoy, 2024).

3.1.1 Defining Cybercrime: An Analytical Approach

Despite its increasing prevalence and global impact, a universally accepted definition of *cybercrime* remains elusive. This definitional ambiguity stems primarily from the inability of scholars and legal practitioners to establish consistent criteria that clearly distinguish cybercrime from conventional forms of criminal activity. The blurred boundaries between traditional crimes and those committed through digital means have made it difficult to create a precise and operational definition.

However, a basic distinction can be established: a criminal act may be classified as a cybercrime if at least one of its essential elements occurs within cyberspace. This view aligns with the analytical model proposed by legal scholar Susan W. Brenner, who conceptualizes the relationship between traditional crime and cybercrime through the following formula (Ajoy, 2024):

Crime + Cyberspace = Cybercrime

This equation suggests that cybercrime is not an entirely new category of offense but rather an evolution of conventional crime facilitated by digital technology and virtual environments.

In traditional criminal law, the two core elements of any offence are mens rea (the guilty mind) and actus reus (the wrongful act). This foundational relationship can be expressed as:

Mens Rea + Actus Reus = Crime

Building on Brenner’s formulation, cybercrime can be analytically represented as:

Cyberspace + (Mens Rea + Actus Reus) = Cybercrime

This equation reflects that, for an offence to qualify as cybercrime, some part of the actus reus must transpire within cyberspace. It is important to note that mens rea—being the mental state or intent of the perpetrator—resides exclusively within the individual and is not inherently linked to the digital environment. As such, mens rea cannot, by its nature, manifest in cyberspace. Therefore, the decisive factor for categorizing an offence as cybercrime is whether the actus reus, or a substantial component thereof, occurs in a virtual setting. To further elucidate this analytical framework, the following two examples are instructive:

a. Consider a scenario in which an offender unlawfully acquires the login credentials of a victim’s online bank account by physically reading them from the victim’s handwritten notes. This initial act of obtaining the credentials constitutes part of the actus reus, yet it occurs in the physical world, not in cyberspace. The perpetrator then uses this information to log into the victim's online bank account and transfer funds to a different account. This subsequent unauthorized transaction takes place within cyberspace. According to the proposed analytical model, the critical component of the actus reus—namely, the unauthorized transfer of money—occurs in a digital environment. Therefore, even though the offence began with a physical act, the defining criminal action transpired online, making the offence a cybercrime under the stated formulation.

b. In another instance, an individual posts a defamatory message on a public platform, such as Instagram, intending to harm the reputation of another person. At first glance, this may appear to be a classic example of cybercrime. However, upon closer examination, it becomes evident that defamation as a legal offence is not complete merely upon posting the message. Defamation is established when a third party reads the content and forms a negative opinion about the victim, resulting in reputational harm. The physical act of typing the message, using a keyboard, and the act of viewing the content by third parties all occur outside cyberspace, using physical devices such as smartphones or computers. While the defamatory content exists in cyberspace as digital data, the impact and interpretation of the content occur in the real world. Consequently, under the proposed analytical framework, this instance does not qualify as cybercrime, because the essential element of actus reus—harmful communication and reputational damage—manifests outside the digital domain. Importantly, the mere presence of evidence (the defamatory post) in cyberspace does not suffice to categorize the act as a cybercrime.

3.1.2 Critical Implications of the Analytical Model

Accepting this refined definition of cybercrime—wherein only those offences with substantive elements of actus reus occurring in cyberspace are included—would have significant implications. It would narrow the scope of cybercrime by excluding certain offences traditionally considered part of this domain, particularly those where digital platforms are incidental rather than integral to the criminal act.

Moreover, the adoption of this analytical model could contribute to greater conceptual clarity and legal precision, particularly in jurisdictional determinations. It would aid in delineating the scope and authority of specialized cybercrime courts or investigative units by ensuring that only offences with a direct digital dimension fall within their remit. This distinction is essential in the development of coherent legal policies and the establishment of targeted enforcement strategies in the digital age.

4. Historical Context of Cybercrime

Human civilization has witnessed a remarkable technological evolution, progressing from primitive calculating tools such as the abacus to the development of modern, high-speed computing systems. This technological transformation, though gradual, has significantly influenced the nature and scope of criminal activity in the digital domain. As computing technologies have advanced, so too have the methods employed by cybercriminals. These actors have continually adapted their techniques to exploit emerging vulnerabilities in digital systems.

Modern cybercriminals increasingly prefer to operate in cyberspace due to several advantages it offers: minimal physical involvement, high financial returns, and, most notably, a reduced risk of identification and apprehension owing to the anonymity afforded by digital environments. In recent decades, cybercrime has evolved into a highly profitable and technologically sophisticated industry, reflecting both the innovation of its perpetrators and the increasing reliance of societies on interconnected digital infrastructures.

Contrary to common belief, cybercrime is not solely a product of the late 20th or early 21st century. Its origins can be traced back to earlier periods in history. This section examines the historical development of cybercrime, beginning with the 19th century and continuing through to the present era, highlighting key events and technological phases that have shaped its evolution.

4.1 The Emergence of Cybercriminal Activities

The first documented instance of cybercriminal activity occurred as early as 1834 in France—long before the development of the Internet or modern computing (RedTeam Cybersecurity Labs, 2023). In this early case, two individuals exploited vulnerabilities in the French telegraph system to gain unauthorized access to financial information, which they then used for market manipulation. Many analysts recognize this as the earliest recorded act resembling cybercrime. It demonstrates that even rudimentary information systems were susceptible to exploitation and that the strategic manipulation of communication technologies for unlawful gain is not a new phenomenon.

From this historical foundation, the development of cybercrime can be divided into four distinct phases, each characterized by the dominant technological infrastructure and the nature of threats posed during that period (Thakre, n.d.).

i. High-Tech Threats of the 1800s

During the late 19th century, email and telegraphic communication represented groundbreaking innovations, enabling more efficient, long-distance correspondence. Though personal computing was not yet prevalent, early mechanisms of information transmission became focal points for criminal manipulation. The emergence of spam-like behavior and identity-related deception—using fictitious identities to gather sensitive information—marked the beginnings of social engineering tactics that would later define modern phishing and fraud schemes.

ii. High-Tech Threats of the 1900s

The 20th century witnessed a dramatic increase in technological advancement, particularly with the rise of personal computers and the proliferation of the Internet. This era saw the emergence of malicious software (malware) such as viruses and worms, which became a major threat to individuals, corporations, and government systems worldwide.

Cybercriminals leveraged web browsers as delivery mechanisms to disseminate self-replicating viruses, which would occupy memory space, disrupt system functionality, or delete critical files. These attacks not only impaired productivity but also caused extensive financial and operational damage. Noteworthy incidents during this era include (RedTeam Cybersecurity Labs, 2023):

- The compromise of the U.S. Air Force's Rome Laboratory by hackers known as Datastream Cowboy and Kuji.
- Vladimir Levin’s cyber intrusion into Citibank’s network, resulting in a high-profile banking theft.
- Max Butler’s extensive hacking activities, which led to one of the longest prison sentences in U.S. cybercrime history.
- The release of the Melissa Virus by David L. Smith, which caused an estimated $80 million in damages.

These events illustrate the rising global visibility and destructiveness of cyber threats in the late 20th century.

iii. High-Tech Threats of the 2000s

The early 21st century saw the mass adoption of social media platforms and digital networking, which significantly increased individuals' exposure to cyber threats. One of the most prevalent forms of cybercrime in this period was identity theft, wherein cybercriminals created fake profiles using stolen personal data—such as photographs and private details—to impersonate victims and commit fraud. This era was also marked by large-scale malware attacks and ransomware outbreaks, including:

- The "I Love You" virus by Onel de Guzman, which caused damages approaching $970 million globally.
- The Code Red and Sasser viruses, which severely disrupted governmental and private networks.
- The Conficker worm, which inflicted an estimated $589.9 billion in damages.
- The WannaCry ransomware attack, which compromised over 230,000 systems worldwide, including hospitals and critical infrastructure.

These incidents underscore the transition of cybercrime from isolated acts to global-scale operations, often involving coordinated efforts and targeting critical digital systems.

iv. High-Tech Threats in the Contemporary Era

In the present day, the rapid proliferation of smartphones and mobile technologies has transformed how individuals communicate, conduct business, and access financial services. With the increasing prevalence of mobile commerce (M-commerce), smartphones have become a central platform for both personal data storage and digital transactions. This shift has made mobile devices primary targets for cybercriminals, who exploit vulnerabilities in mobile operating systems, unsecured applications, and poorly protected wireless networks.

One of the most pressing concerns in the current digital environment is the theft of sensitive financial and personal information from smartphones. Cybercriminals often exploit weak legal protections and insufficient security protocols surrounding mobile transactions. Furthermore, the demographic most affected by such attacks tends to be younger users, who frequently engage in mobile banking and e-commerce without fully understanding the associated risks.

Despite the increasing sophistication of cyber threats, legislative and institutional responses to mobile-based cybercrime remain underdeveloped in many jurisdictions, creating a legal vacuum that emboldens perpetrators and challenges law enforcement agencies.

5. Major Categories of Cybercrime on Social Media in Pakistan

Social media has emerged as one of the most prevalent and influential forms of digital interaction in the 21st century. On average, users now dedicate approximately two hours and twenty-four minutes daily to various social networking platforms (Almadhoor, Alserhani, & Humayun, 2021). These platforms, grounded in technological innovations, facilitate real-time communication, content sharing, and knowledge exchange among individuals across the globe. The most commonly used social media applications in Pakistan include WhatsApp, YouTube, Facebook, TikTok, Instagram, Twitter (X), LinkedIn, Messenger, and Telegram (Anudini, Dissanayake, & Uwanthika, 2021).

While these platforms provide numerous societal and economic benefits, their interactive and open-access nature has simultaneously rendered them vulnerable to exploitation by cybercriminals. The increased reliance on digital communication has expanded the attack surface for malicious actors, making social networks a fertile ground for cybercrime. Offenders exploit these platforms to acquire personal data, manipulate users, and engage in illicit digital activities. Cybercrimes conducted through or against computers generally fall into three overarching categories (Kamran, Arafeen, & Shaikh, 2019):

a. **Crimes where computers are the direct target**, such as hacking, data breaches, and malware attacks;
b. **Crimes where computers serve as a medium**, such as fraud, child pornography, and illegal dissemination of personal data; and
c. **Crimes where computers are used as storage or repositories**, such as hosting illegal information or stolen data.

In the context of Pakistan, the National Response Centre for Cyber Crime (NR3C) has classified cyber offences on social media into six major categories: malware attacks, identity theft, social engineering/phishing, cyberstalking, burglary via social networks, and cyber-casing (Soomro & Hussain, 2019). Each of these categories reflects the evolving nature of cybercrime and its impact on the Pakistani digital ecosystem. A more detailed analysis of these categories is as follows:

5.1 Phishing and Social Engineering

Social engineering refers to the act of manipulating individuals into divulging confidential information. Phishing, a subset of social engineering, involves the fraudulent impersonation of legitimate entities through email, messaging, or social media platforms (Saleem et al., 2022). The perpetrator constructs counterfeit websites or pages that closely resemble authentic platforms, such as banking sites or social networks like Facebook, to deceive users into entering sensitive information such as login credentials, passwords, or credit card numbers.

One common form of phishing in Pakistan involves users receiving urgent financial requests via messages that appear to originate from friends or family. However, these messages are often sent by cybercriminals who have compromised the victim's account. According to cybersecurity firm Trend Micro, Facebook is particularly vulnerable due to its wide user base and simple user interface, which facilitates deception. The rapid and effective nature of phishing makes it one of the most widespread and successful forms of cybercrime on Pakistani social media.

5.2 Hacking

Hacking is defined as the unauthorized intrusion into a computer system or network with the intent to access, modify, or steal data. On social media platforms, hacking typically involves compromising user accounts to gain control over their digital identity, send malicious messages, or extract sensitive information (Akhlaq, 2021).

In Pakistan, hacking incidents have targeted not only individuals but also financial institutions. The NR3C 2018 report revealed significant breaches in Pakistani banking systems, with hackers reportedly selling the data of over 8,000 account holders from 10 local banks. Furthermore, in April 2019, cybercriminals orchestrated a heist involving the theft of 16 million Pakistani rupees from bank accounts belonging to exporters based in Sialkot (Kanwal, 2023). These examples underscore the scale and severity of hacking-related offences, which range from personal account thefts to large-scale corporate and financial intrusions.

5.3 Malicious Software (Malware)

Malware, or malicious software, is a type of harmful program designed to damage, disrupt, or gain unauthorized access to computer systems (Anudini et al., 2021). On social media, malware is often embedded in links, attachments, and messages, thereby exploiting user trust and platform vulnerabilities. When users inadvertently click on such links or open malicious attachments, malware infiltrates their devices and may execute actions such as data theft, surveillance, encryption for ransom, or system sabotage. Three of the most common types of malwares affecting social media users are (Almadhoor et al., 2021):

a. **Cross-site scripting (XSS)**, which injects malicious scripts into trusted websites;
b. **Trojans**, which disguise themselves as legitimate software but act as backdoors for hackers; and
c. **Clickjacking**, where users are tricked into clicking on concealed malicious links.

The widespread sharing nature of social media contributes to the rapid propagation of malware, increasing its reach and impact across user networks.

5.4 Identity Theft

Identity theft involves the unauthorized acquisition and misuse of another person's Personally Identifiable Information (PII), such as names, national identity numbers, financial records, and images. On social media, perpetrators may impersonate users by creating fake profiles, stealing personal photographs, or accessing private information to commit fraud, apply for credit, or conduct scams (Anudini et al., 2021). The major types of identity theft include:

a. **Financial identity theft**, where stolen data is used to obtain loans or make purchases;
b. **Medical identity theft**, where individuals use another person’s identity to obtain healthcare services or insurance;
c. **Child identity theft**, which involves using a minor’s information to create fraudulent accounts; and
d. **Criminal identity theft**, where offenders use another person’s identity to evade law enforcement.

This form of cybercrime poses severe threats to the financial integrity and psychological well-being of the victims, particularly when it results in legal or economic repercussions.

5.5 Spamming

Spamming refers to the excessive or unsolicited transmission of identical or irrelevant messages, links, advertisements, or content on social media platforms. Originally confined to emails, spam has now permeated mainstream social media environments, often serving as a vehicle for phishing schemes, malware dissemination, or online fraud.

Spammers exploit the architecture of social platforms to spread deceptive content that may redirect users to compromised websites. Clicking these links can trigger data breaches, install spyware, or harvest user credentials. Although often perceived as a nuisance, spamming serves as a gateway for more complex cybercrimes, contributing to financial losses and compromising user privacy.

5.6 Cyberbullying and Cyber Harassment

Cyberbullying and cyber harassment represent significant digital threats in Pakistan, disproportionately affecting women, adolescents, and minority communities. These acts involve the intentional use of digital technologies to intimidate, threaten, or humiliate individuals, often through messages, comments, or posts intended to cause psychological harm (Bhatti, 2022). Forms of cyber harassment include: hate speech, sexual extortion (sextortion), trolling and public shaming, persistent stalking, and Impersonation and fake accounts.

According to the Digital Rights Foundation (DRF), from December 2016 to 2023, its Cyber Harassment Helpline received 16,849 complaints from across Pakistan. In 2023 alone, 2,473 new cases were reported, with women constituting 58.5% of the complainants, underscoring the gendered dimension of digital abuse. Furthermore, it is estimated that 40% of Pakistani women who use the Internet experience some form of cyber harassment, particularly on platforms like Facebook, WhatsApp, and Messenger (The Reporters, 2024).

5.7 Cyberstalking

Cyberstalking involves the persistent and unwanted surveillance, contact, or harassment of individuals through digital platforms (Soomro & Hussain, 2019). Unlike general online harassment, cyberstalking is continuous and intentional, with the aim of instilling fear, anxiety, or emotional distress in the victim. Cyberstalking may include: threatening messages, repeated unsolicited communication, sharing explicit or invasive content and impersonation or location tracking.

According to NR3C, cyberstalking is distinct from identity theft in that it involves a conscious awareness of harm. While identity thieves are primarily motivated by financial gain and often indifferent to the consequences for victims, cyberstalkers are psychologically invested in the emotional impact of their actions, often pursuing personal vendettas or control over their targets.

6. Conclusion

In conclusion, the term *cybercrime*—derived from the combination of the words *cyber* and *crime*—encompasses a broad spectrum of unlawful acts committed through or facilitated by digital technologies. The concept of cybercrime maintains a close conceptual and functional connection with conventional criminal law, as both involve human conduct that violates legal norms and is punishable by the state. Foundational jurists such as John Austin, Jeremy Bentham, Glanville Williams, J.W. Cecil Turner, and authorities like *Halsbury's Laws of England* have offered various definitions of crime, each highlighting the essential features of wrongful conduct, state recognition, and penal sanction. A comprehensive understanding of cybercrime thus necessitates a prior grasp of the classical notion of crime. Cybercrime, as a contemporary construct, has largely replaced earlier terminology such as "computer crime." It refers to deliberate actions carried out via digital means—particularly the Internet and mobile technologies—with the intention to harm, defraud, or disrupt individuals or systems. These acts may target reputation, inflict emotional or physical distress, or compromise financial and informational security.

Pakistan, due to its expanding digital landscape and rapidly growing number of internet and social media users, is particularly susceptible to cyber threats. Social media, in particular, has become a prominent vector for cybercrime due to its widespread use, accessibility, and data-rich environment. Cybercriminals exploit these platforms to gain unauthorized access to personal information, propagate malicious content, and commit a range of digital offences. The most prevalent forms of cybercrime affecting Pakistani users on social networking platforms include phishing, hacking, the dissemination of malware, identity theft, spamming, cyberbullying, and cyberstalking. These activities not only pose technological risks but also threaten the social, psychological, and financial well-being of individuals. Incidents of online harassment, defamation, financial fraud, and data breaches are steadily increasing, particularly targeting vulnerable groups such as women and minors.

Given the severity and scope of cybercrime on social media in Pakistan, there is a pressing need for comprehensive legal frameworks, enhanced digital literacy, and robust cybersecurity mechanisms. A multi-stakeholder approach—encompassing legislative reform, institutional enforcement, public awareness, and private sector cooperation—is essential to mitigate the harmful consequences of cybercrime and protect individuals' rights in the digital sphere.

References:

Ajoy, P. B. (2024). Developing an analytical definition of cybercrime. *Journal of Humanities and Social Science, 29*(1), 12–19. https://papers.ssrn.com/abstract=4701799

Akhlaq, M. (2021). Cybercrime in Pakistan: A study of the law dealing with cybercrimes in Pakistan. *PCL Student Journal of Law, 5*(1). LEAP Pakistan. https://leappakistan.com/pclsjl-vol-5-issue-1-2021/

Almadhoor, L., Alserhani, F., & Humayun, M. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education, 12*, 2972–2981. https://turcomat.org/index.php/turkbilmat/article/view/4947

Anudini, A., Dissanayake, H. M. S. S., & Uwanthika, G. A. I. (2021). *Impact of social media-related cybercrimes and preventive precautions*. http://ir.kdu.ac.lk/handle/345/5230

Bhatti, H. (2022). The case of cyberbullying in Pakistan. *Paradigm Shift*. https://www.paradigmshift.com.pk/cyberbullying-in-pakistan/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*(1), 13–20. http://link.springer.com/10.1007/s11416-006-0015-z

Goswami, S., & Goswami, P. S. (2024). *Cyber crimes and laws*. BFC Publications.

Haider, W., Ali, A., & Zubair, M. (2023). Prevention of Electronic Crime Act, 2016: An analysis of the act's effectiveness in controlling misuse of social media in Pakistan. *Journal of Educational Research & Social Sciences Review*. https://ojs.jerssr.org.pk/index.php/jerssr/article/view/197

Hooker, M. P. (2019). Censorship, free speech & Facebook: Applying the First Amendment to social media platforms via the public function exception. *Washington Journal of Law, Technology & Arts, 15*(1), 36. https://digitalcommons.law.uw.edu/wjlta/vol15/iss1/3

Hussain, F., & Qureshi, B. (2018). Social media and policy making in Pakistan. *Pakistan Administrative Review, 2*(1), 208–221. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-56902-0

Kamran, A., Arafeen, Q. ul, & Shaikh, A. A. (2019). Existing cyber laws and their role in legal aspects of cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics, 8*(3), 241–250. https://www.researchgate.net/publication/338885893_Existing_Cyber_Laws_and_Their_Role_in_Legal_Aspects_of_Cybercrime_in_Pakistan

Kemp, S. (2024, February 23). *Digital 2024: Pakistan*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2024-pakistan

Khalmuratov, A. O. (2024). Genesis of cybercrime and its concept peculiarities. *International Journal of Law and Criminology, 4*(2), 116–120. https://doi.org/10.37547/ijlc/Volume04Issue02-20

National Response Centre for Cyber Crime. (n.d.). *Cybercrime*. https://www.nr3c.gov.pk/cybercrime.html

RedTeam Cybersecurity Labs. (2023). *A brief history of cybercrime*. https://theredteamlabs.com/a-brief-history-of-cybercrime/

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1–9). IEEE. https://ieeexplore.ieee.org/abstract/document/7740434/

Saleem, H., Jan, J., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Society, Law and Policy Review, 1*(1), 10–22. https://doi.org/10.62585/slpr.v1i1.21

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems, 24*(1), 9–17. https://sciendo.com/article/10.2478/acss-2019-0002

Thakre, A. G. (n.d.). *Cyber crime: History & evolution*. e-PG Pathshala. https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=MVs9IY38j6bxSw+ryrjUow==

The Reporters. (2024). *DRF cyber harassment helpline report: Rise in online violence*. https://thereporters.pk/drf-cyber-harassment-helpline-report-rise-in-online-violence/

Tiwari, S., & Ghosh, G. (2014). *Social media and freedom of speech and expression: Challenges before the Indian law*. https://papers.ssrn.com/abstract=2892537

United Nations. (2000). *Crimes related to computer networks*. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf