Cyber Laws

By

SHAHID NAEEM

(Gold Medalist)

M.Sc. (Eco), MA(Pol.Sci), MCS, LL.M., DLL

Advocate High Court

Principal Kings Law College,

Sheikhupura.

INTRODUCTION TO CYBER CRIMES

Q.	Define Cyber Crime. Discuss its nature, scope, and the various classifications of crimes committed in cyberspace.

Ans:

Introduction
Cyber crime is one of the fastest-growing forms of criminal activity in the modern digital world. With the increasing use of the internet, smartphones, and computer systems in Pakistan, almost every aspect of life—such as education, banking, communication, and business—has shifted online. While this digital transformation has created convenience and efficiency, it has also opened new doors for criminals to exploit weaknesses in information systems. Cyber crime is not limited by physical boundaries and can be committed remotely with little risk of immediate detection. Therefore, it is very important for law students to understand its meaning, characteristics, scope, and different forms in detail.

Definition of Cyber Crime

Cyber crime refers to any illegal activity that is carried out using a computer, digital device, or internet, where the computer, data, or network is used as a tool, target, or place of the offence. It includes a wide range of acts such as hacking, online fraud, identity theft, cyber stalking, and spreading harmful or illegal content.

This definition shows that cyber crime is not limited to a single type of offence but covers many unlawful acts involving digital technology. Under the **Prevention of Electronic Crimes Act, 2016 (PECA)**, actions like unauthorized access to data, electronic fraud, cyber terrorism, and offences against dignity are clearly recognized as cyber crimes .

Example:
If a person gains access to another person's email account without permission and reads or deletes messages, it is considered a cyber crime because it involves unauthorized access to an information system.

NATURE OF CYBER CRIME

The nature of cyber crime explains its basic characteristics and highlights how it differs from traditional crimes. These features help in understanding why cyber crime is difficult to control and investigate.

1. Borderless and Global Nature

Cyber crime is not restricted to any specific country or region. It can be committed from any part of the world and can affect victims located in different countries at the same time. This makes jurisdiction and enforcement of laws more complicated.

Example:
A hacker sitting in Europe can attack a Pakistani company's database and steal sensitive information without ever visiting Pakistan.

2. Anonymity of the Offender

One of the most important features of cyber crime is that criminals can easily hide their identity. They use fake names, encrypted networks, or tools like VPNs to remain anonymous.

This anonymity creates serious challenges for law enforcement agencies in identifying and prosecuting offenders.

Example:
A person creates multiple fake social media accounts to threaten or blackmail someone, making it difficult to trace the real person behind those accounts.

3. Technical and Complex Nature

Cyber crimes often involve advanced technical knowledge of computers, networks, and software systems. The complexity of these crimes makes investigation and prosecution more difficult compared to traditional crimes.

Example:
A cyber criminal develops a virus or malware that spreads through emails and damages computer systems of users.

4. High Speed and Large-Scale Impact

Cyber crimes can be committed very quickly and can affect a large number of people at once. Unlike traditional crimes, which may target one victim at a time, cyber crimes can target thousands of victims simultaneously.

Example:
A phishing attack where thousands of emails are sent within seconds to trick users into sharing their bank details.

5. Non-Physical Nature

Cyber crimes do not involve physical force or direct contact with the victim. However, they can still cause serious harm such as financial loss, emotional distress, and damage to reputation.

Example:
Posting false allegations about a person on social media can harm their reputation without any physical interaction.

6. Continuous Evolution

Cyber crime is constantly changing as new technologies are developed. Criminals continuously find new methods and tools to commit offences, making it difficult for laws to keep up.

Example:
Earlier, fraud was mainly done through emails, but now criminals use fake mobile applications and social media platforms for scams.

SCOPE OF CYBER CRIME

The scope of cyber crime is very broad because it affects different areas of society, including individuals, businesses, governments, and the overall social system. Its impact is increasing day by day with the growth of digital technology.

1. Scope in Relation to Individuals

Cyber crime has a direct impact on individuals by violating their privacy, security, and dignity. Personal information can be easily stolen or misused online.

Example:
A person's CNIC number or personal photos are stolen and used for illegal purposes such as blackmail or fraud.

2. Scope in Relation to Businesses and Organizations

Businesses rely heavily on digital systems for their operations. Cyber attacks can result in loss of confidential data, financial loss, and damage to reputation.

Example:
Hackers break into a company's database and steal customer records, which are then sold on the dark web.

3. Scope in Relation to Government and State

Cyber crime can also target government institutions and threaten national security. Attacks on government systems can disrupt public services and create instability.

Example:
Hackers attack a government website and leak sensitive official information.

4. Scope in Financial Sector

Financial institutions such as banks are major targets of cyber criminals. Online banking systems are often attacked for financial gain.

Example:
A fraudster sends fake messages pretending to be a bank and tricks users into sharing their ATM PINs.

5. Social and Moral Scope

Cyber crime affects society by spreading harmful content, fake news, and immoral material. This can disturb social harmony and public order.

Example:
Spreading false rumors on social media that create fear or conflict among people.

CLASSIFICATION OF CYBER CRIMES

Cyber crimes can be divided into different categories based on their target and nature. This classification helps in understanding the different types of offences and their legal treatment.

1. Crimes Against Individuals

These crimes directly target individuals and affect their privacy, dignity, and personal security. Such crimes are very common in the digital age due to the widespread use of social media.

- Cyber stalking
- Identity theft
- Cyberbullying
- Online harassment
- Defamation

Example:
Sending repeated threatening messages to a person on social media or sharing their private photos without consent.

2. Crimes Against Property

These crimes involve damage to or theft of digital property such as data, software, or intellectual property. They are often committed for financial gain or revenge.

- Hacking
- Data theft
- Malware attacks (viruses, ransomware)
- Software piracy

Example:
A hacker installs ransomware in a company's system and demands money to restore access to important files.

3. Crimes Against Organizations

These crimes target companies, institutions, or networks, often causing disruption in their operations and financial loss.

- Denial of Service (DoS) attacks
- Data breaches

- Corporate espionage

Example:
Attackers flood a company's website with traffic so that legitimate users cannot access it.

4. Crimes Against Society

These crimes affect society as a whole by disturbing peace, morality, and public order. They often involve misuse of online platforms to spread harmful content.

- Hate speech
- Fake news
- Online gambling
- Distribution of illegal content

Example:
Posting content that promotes religious hatred and leads to social unrest.

5. Crimes Against State

These are serious offences that threaten the security and sovereignty of a country. Such crimes are often dealt with strictly under the law.

- Cyber terrorism
- Espionage
- Attacks on critical infrastructure

Example:
Hacking military communication systems or government databases.

6. Financial Cyber Crimes

These crimes are committed with the aim of gaining money illegally through digital means. They are very common due to the rise of online banking and e-commerce.

- Electronic fraud
- Phishing
- Credit card fraud
- Online scams

Example:
Sending emails that appear to be from a bank and asking users to enter their login credentials.

7. Content-Based Cyber Crimes

These crimes involve the creation, distribution, or possession of illegal or harmful digital content. They are strictly prohibited under cyber laws.

- Child pornography

- Obscene content
- Cyberbullying material

Example:
Uploading or sharing inappropriate videos involving minors, which is a serious offence under PECA.

Conclusion

Cyber crime is a complex and ever-growing issue in the digital world. It includes a wide range of illegal activities carried out through computers and the internet, affecting individuals, organizations, and governments. Its unique nature, such as anonymity, global reach, and rapid execution, makes it more challenging to control compared to traditional crimes. The scope of cyber crime continues to expand with technological advancements, increasing the need for effective legal frameworks like the Prevention of Electronic Crimes Act, 2016 in Pakistan. Understanding its nature, scope, and classification helps law students and legal professionals to better address cyber offences and contribute to maintaining law and order in cyberspace.

Q.	Explain the historical evolution of Cyber Laws in Pakistan, specifically focusing on the transition from the Electronic Transactions Ordinance (ETO) to the Prevention of Electronic Crimes Act (PECA).

Ans:

Introduction
The historical development of cyber laws in Pakistan shows how the legal system has gradually adapted to the challenges created by modern technology. In the early years, there were no specific laws to deal with issues arising from the use of computers and the internet. As digital communication, e-commerce, and online services expanded, new legal problems emerged, including electronic fraud, hacking, and misuse of personal data. To respond to these challenges, Pakistan first introduced the Electronic Transactions Ordinance (ETO) in 2002, which mainly focused on giving legal recognition to electronic records. However, due to the rapid rise in cyber crimes, a more comprehensive law became necessary, leading to the enactment of the Prevention of Electronic Crimes Act (PECA) in 2016.

Historical Evolution of Cyber Laws in Pakistan

The evolution of cyber laws in Pakistan can be divided into different stages, each reflecting the technological and social developments of its time. Initially, there was no specialized legislation to deal with cyber-related issues. Traditional laws such as the Pakistan Penal Code, 1860 were applied to certain situations, but these laws were not designed for digital environments and often failed to address the complexities of cyber crime.

As the use of computers and the internet increased in Pakistan during the late 1990s and early 2000s, the government realized the need for a proper legal framework. The first step was to facilitate electronic transactions and provide legal recognition to digital communication. This

led to the introduction of ETO in 2002. However, with the growth of social media, online banking, and digital platforms, new forms of crimes emerged, which required stronger legal measures. This eventually resulted in the development of PECA 2016, which is a more detailed and comprehensive cyber law.

Electronic Transactions Ordinance (ETO), 2002

The Electronic Transactions Ordinance, 2002 was the first formal attempt by Pakistan to regulate activities in cyberspace. It was mainly designed to support the growth of e-commerce and digital communication by recognizing electronic records and signatures.

This law marked the beginning of cyber law in Pakistan, but its primary focus was not on criminal activities. Instead, it aimed to create trust in electronic transactions and encourage businesses and individuals to use digital platforms.

Purpose of ETO, 2002

The main purpose of ETO was to remove legal uncertainties related to electronic communication and transactions. Before this law, electronic documents and online agreements were not clearly recognized under Pakistani law, which created problems for businesses and individuals.

ETO aimed to ensure that electronic records would be treated equally with paper-based documents. It also sought to promote confidence in online transactions by providing a legal framework for digital signatures and authentication.

Example:
If two parties entered into a contract through email, ETO ensured that such a contract would be legally valid and enforceable in court.

Key Features of ETO, 2002

1. Legal Recognition of Electronic Documents

ETO provided that electronic documents, records, and communications would have the same legal status as traditional paper documents. This was a significant step in promoting digital communication.

This provision made it easier for businesses to operate online and reduced the need for physical documentation.

Example:
An online invoice or digital receipt issued by a company became legally acceptable proof of transaction.

2. Recognition of Digital Signatures

ETO recognized digital signatures as a valid method of authentication. This helped in verifying the identity of parties involved in electronic transactions.

Digital signatures increased trust and security in online dealings.

Example:
A company could sign contracts digitally using secure encryption methods instead of handwritten signatures.

3. Establishment of Certification Authorities

ETO allowed for the establishment of certification authorities responsible for issuing and verifying digital certificates. These authorities ensured that digital signatures were authentic and secure.

This mechanism played an important role in building confidence in electronic transactions.

4. Facilitation of E-Commerce

By providing legal recognition to electronic transactions, ETO encouraged the growth of e-commerce in Pakistan. Businesses could now operate online without fear of legal uncertainty.

Example:
Online shopping platforms could legally process orders and payments through digital systems.

Limitations of ETO, 2002

Despite its importance, ETO had several weaknesses that limited its effectiveness in dealing with cyber crime.

Firstly, it focused mainly on civil matters such as electronic contracts and did not adequately address criminal activities in cyberspace. Secondly, it lacked clear definitions and punishments for offences like hacking, identity theft, and online fraud. Thirdly, it did not provide proper investigation procedures or enforcement mechanisms.

As technology advanced, these limitations became more serious, highlighting the need for a new and comprehensive law.

Example:
If someone hacked into a system or committed online fraud, ETO did not clearly define such acts as offences or provide punishments, making it difficult to take legal action.

Cyber Laws

Need for Transition from ETO to PECA

With the rapid increase in internet users, mobile technology, and social media platforms in Pakistan, cyber crimes started increasing at an alarming rate. New types of crimes such as cyber stalking, online harassment, phishing, and cyber terrorism emerged, which were not covered under ETO.

The absence of a strong legal framework created difficulties for law enforcement agencies in investigating and prosecuting cyber criminals. There was also a growing need to protect individuals' privacy, secure financial systems, and ensure national security.

Therefore, it became necessary to introduce a new law that could comprehensively deal with cyber crimes, provide clear definitions, prescribe punishments, and establish proper investigation procedures. This led to the enactment of PECA in 2016.

Prevention of Electronic Crimes Act (PECA), 2016

The Prevention of Electronic Crimes Act, 2016 is a comprehensive law designed to address various forms of cyber crime in Pakistan. It not only defines offences but also provides mechanisms for their prevention, investigation, and punishment.

PECA represents a major shift in Pakistan's legal approach by focusing specifically on criminal activities in cyberspace and ensuring protection for individuals, organizations, and the state .

Purpose of PECA, 2016

The main purpose of PECA is to prevent unauthorized acts related to information systems and to provide a legal framework for dealing with cyber offences. It aims to protect data, ensure privacy, and maintain the integrity of digital systems.

In addition, PECA seeks to create a safe online environment by addressing issues such as harassment, fraud, and misuse of information.

Example:
If someone steals another person's personal data and uses it for fraud, PECA provides legal provisions to punish the offender.

Key Features of PECA, 2016

1. Comprehensive Coverage of Cyber Offences

PECA defines a wide range of cyber crimes, including unauthorized access, data interference, electronic fraud, identity theft, cyber stalking, and cyber terrorism.

This comprehensive approach ensures that most forms of cyber crime are covered under the law.

Example:
Accessing someone's social media account without permission is clearly defined as an offence.

2. Prescribed Punishments and Penalties

PECA provides specific punishments for different offences, including imprisonment and fines. The severity of punishment depends on the nature of the crime.

This helps in creating deterrence and discouraging individuals from committing cyber crimes.

Example:
Electronic fraud can result in imprisonment along with financial penalties.

3. Investigation Powers and Procedures

PECA gives authority to investigation agencies to collect digital evidence, conduct searches, and seize data. It also provides procedures for handling cyber crime cases.

This ensures that offences can be properly investigated and prosecuted.

Example:
Law enforcement agencies can trace IP addresses and recover deleted data during investigations.

4. Protection of Individuals' Rights

PECA includes provisions to protect individuals from online harassment, blackmail, and misuse of personal information. It recognizes offences against dignity and privacy.

Example:
Cyber stalking and online harassment are punishable under PECA.

5. Protection of National Security

The law addresses serious threats such as cyber terrorism and attacks on critical infrastructure, which can affect national security.

Example:
Hacking into government systems or spreading terrorist content online is treated as a serious offence.

6. Regulation of Online Content

PECA allows authorities to remove or block unlawful and harmful online content. This helps in controlling the spread of fake news, hate speech, and illegal material.

Example:
Content promoting violence or hatred can be blocked by authorities.

7. International Cooperation

PECA also provides for cooperation with other countries in dealing with cyber crimes, recognizing the global nature of such offences.

This is important because many cyber crimes involve cross-border elements.

Transition from ETO to PECA

The transition from ETO to PECA represents a significant development in Pakistan's cyber law framework. It shows how the legal system evolved from basic regulation of electronic transactions to comprehensive control of cyber crimes.

1. Shift from Civil to Criminal Focus

ETO mainly dealt with civil aspects such as contracts and transactions, while PECA focuses on criminal offences and their punishment. This shift reflects the increasing importance of addressing cyber crime.

2. Expansion of Legal Scope

ETO had a limited scope, whereas PECA covers a wide range of offences affecting individuals, organizations, and the state. This expansion makes PECA a more effective law.

3. Introduction of Enforcement Mechanisms

ETO lacked proper enforcement provisions, but PECA provides detailed procedures for investigation, prosecution, and trial of cyber offences.

4. Response to Technological Advancement

PECA addresses modern cyber threats such as social media misuse, online fraud, and cyber terrorism, which were not considered under ETO.

5. Strengthening Legal Protection

PECA offers stronger protection to individuals, businesses, and government institutions by clearly defining offences and prescribing punishments.

Example:
Under ETO, hacking was not clearly punishable, but under PECA, it is a defined offence with strict penalties.

Conclusion

The historical evolution of cyber laws in Pakistan highlights the country's efforts to adapt its legal system to the challenges of the digital age. The Electronic Transactions Ordinance, 2002 laid the foundation by recognizing electronic records and promoting e-commerce, but it was

limited in addressing cyber crime. With the rapid growth of technology and increasing cyber threats, the need for a more comprehensive law became evident. The Prevention of Electronic Crimes Act, 2016 fulfilled this need by providing detailed definitions, punishments, and enforcement mechanisms for cyber offences. This transition represents a significant step towards ensuring security, privacy, and legal protection in Pakistan's digital environment.

Q. What is **Critical Infrastructure**? Elaborate on the legal protections provided for critical infrastructure under Pakistani law. **(Imp)**

Ans:

Introduction
In the modern digital age, the functioning of a state depends heavily on its critical infrastructure, which includes essential systems such as energy, communication, banking, transportation, and government networks. These systems are increasingly operated through information technology and interconnected digital platforms, making them vulnerable to cyber attacks. Any disruption to such infrastructure can cause serious consequences, including economic loss, public panic, and threats to national security. Therefore, protecting critical infrastructure has become a major concern for governments around the world, including Pakistan. Pakistani cyber law, especially the Prevention of Electronic Crimes Act (PECA), 2016, provides important legal protections to safeguard such infrastructure from cyber threats.

Definition of Critical Infrastructure

Critical infrastructure refers to those essential systems, facilities, and networks whose disruption or destruction would have a serious impact on national security, economy, public safety, or the functioning of the state.

Under PECA 2016, critical infrastructure includes assets, systems, or networks, the loss or compromise of which can result in major damage to essential services or national security .

This definition shows that critical infrastructure is not limited to physical structures but also includes digital systems and data that support essential services.

Example:
Electric power grids, banking systems, telecommunication networks, and government databases are all considered critical infrastructure.

Nature and Importance of Critical Infrastructure

Critical infrastructure plays a vital role in maintaining the stability and security of a country. Its proper functioning ensures that essential services are continuously available to the public.

Any attack on such infrastructure can disrupt daily life, create panic, and even threaten the sovereignty of the state. Therefore, it is considered a high-priority area for legal protection.

Example:
If a cyber attack shuts down a country's electricity system, hospitals, transport, and communication networks may stop functioning, leading to a national crisis.

Types of Critical Infrastructure

Critical infrastructure covers a wide range of sectors that are essential for the functioning of a state and the well-being of its citizens. These sectors are interconnected, meaning that a failure in one sector can directly affect others. In Pakistan, both physical facilities and digital systems that support essential services are considered part of critical infrastructure. Understanding these types helps in identifying areas that require strong legal protection.

1. Energy Sector

The energy sector is one of the most important components of critical infrastructure because it supports almost all other sectors. It includes electricity generation, transmission, and distribution systems, as well as oil and gas facilities.

A disruption in the energy sector can bring the entire country to a standstill, affecting hospitals, industries, communication systems, and daily life activities.

Example:
If hackers attack a power grid and cause a nationwide blackout, hospitals may lose power, industries may stop production, and communication systems may fail.

2. Financial Sector

The financial sector includes banks, stock exchanges, insurance companies, and online payment systems. In today's digital age, most financial transactions are conducted electronically, making this sector highly dependent on information systems.

Any cyber attack on this sector can result in huge financial losses and loss of public trust in the banking system.

Example:
If a cyber criminal hacks into a bank's system and transfers money illegally, it can affect thousands of customers and damage the reputation of the bank.

3. Telecommunication Sector

This sector includes mobile networks, internet service providers, satellite communication systems, and other communication technologies. It plays a key role in connecting people, businesses, and government institutions.

Since communication systems are essential for coordination and emergency response, their disruption can create serious problems.

Example:
If a cyber attack shuts down mobile networks, people will not be able to communicate during emergencies, and businesses may suffer losses.

4. Transportation Sector

The transportation sector includes air traffic control systems, railway networks, shipping systems, and road traffic management systems. These systems rely heavily on digital technology for smooth operation.

A cyber attack on transportation systems can lead to accidents, delays, and disruption of supply chains.

Example:
If hackers interfere with railway signaling systems, it may lead to train accidents or major delays.

5. Government and Public Sector Systems

This includes government databases, public administration systems, and digital services provided by the state. These systems store sensitive information about citizens and are essential for governance.

Any breach of such systems can compromise national security and public trust.

Example:
Unauthorized access to a national identity database can lead to misuse of citizens' personal information.

6. Defense and National Security Systems

Defense systems include military communication networks, intelligence systems, and strategic control systems. These are among the most sensitive parts of critical infrastructure.

Any attack on these systems can directly threaten the sovereignty and security of the state.

Example:
Hacking into military communication systems can disrupt defense operations and expose confidential information.

7. Health Sector

The health sector includes hospitals, medical databases, and emergency response systems. Modern healthcare relies heavily on digital systems for patient records and treatment processes.

A cyber attack on this sector can risk human lives.

Example:
If hospital systems are hacked and patient records are altered or deleted, doctors may not be able to provide proper treatment.

8. Water and Utilities Sector

This sector includes water supply systems, sewage systems, and other public utilities. These systems are essential for public health and daily life.

Disruption in these services can create serious health and environmental problems.

Example:
If a cyber attack contaminates or disrupts a city's water supply system, it can lead to a public health crisis.

Legal Protections for Critical Infrastructure under Pakistani Law

Pakistani law, particularly the Prevention of Electronic Crimes Act (PECA), 2016, provides strong legal protections to safeguard critical infrastructure from cyber threats. These protections are designed to prevent unauthorized access, ensure system security, and punish offenders who attempt to damage essential systems.

1. Criminalization of Unauthorized Access to Critical Systems

PECA makes it a criminal offence to access any information system or data without authorization, especially when it relates to critical infrastructure.

This provision is important because it protects sensitive systems from hackers and unauthorized users.

Example:
If a person attempts to gain access to a government server or power grid system without permission, it is a punishable offence.

2. Protection Against Unauthorized Copying and Data Theft

The law prohibits copying, transmitting, or stealing data from critical infrastructure systems without permission. This helps in protecting confidential and sensitive information.

This is particularly important for sectors like banking, defense, and government databases.

Example:
Stealing confidential defense data or financial records from a secure system is a serious cyber crime.

3. Protection Against Interference and Damage

Any act that interferes with or damages an information system, including making it unavailable or altering its functioning, is prohibited under PECA.

This ensures that critical systems continue to operate smoothly without disruption.

Example:
Launching a Distributed Denial of Service (DDoS) attack on a banking system to shut it down is an offence.

4. Special Protection for Critical Infrastructure (Enhanced Punishments)

PECA provides stricter punishments for offences related to critical infrastructure compared to ordinary cyber offences. This reflects the importance of these systems for national security and public safety.

This enhanced protection acts as a strong deterrent against potential attackers.

Example:
Hacking into a personal computer may carry a lighter penalty, but hacking into a national power grid system results in more severe punishment.

5. Criminalization of Cyber Terrorism

Cyber terrorism is one of the most serious offences under PECA. It includes attacks on critical infrastructure intended to create fear, panic, or harm to the state.

This provision ensures that large-scale cyber attacks are dealt with strictly.

Example:
Attacking a country's electricity or defense system to create chaos among the public is considered cyber terrorism.

6. Investigation Powers and Digital Forensics

PECA grants powers to authorized agencies to investigate cyber crimes involving critical infrastructure. These powers include search, seizure, and analysis of digital evidence.

This helps in identifying offenders and collecting proof for prosecution.

Example:
Authorities can seize computers used in a cyber attack and analyze them to trace the source of the attack.

7. Data Integrity and Confidentiality Protection

The law ensures that data related to critical infrastructure remains accurate, secure, and protected from unauthorized changes or disclosure.

Maintaining data integrity is essential for the proper functioning of systems.

Example:
Altering financial data in a banking system to transfer funds illegally is a serious offence.

8. Real-Time Monitoring and Prevention Measures

PECA allows for real-time collection and monitoring of data in certain cases to prevent cyber attacks on critical infrastructure.

This helps in detecting threats before they cause damage.

Example:
Monitoring network activity to detect suspicious behavior and prevent a cyber attack on a government system.

9. International Cooperation

Since cyber attacks can originate from outside Pakistan, PECA provides for cooperation with other countries in investigation and prevention.

This is essential for dealing with cross-border cyber crimes.

Example:
If a cyber attack on Pakistan's infrastructure originates from another country, authorities can cooperate with that country to identify and arrest the offender.

Conclusion

Critical infrastructure is the backbone of any modern state, as it supports essential services and ensures the smooth functioning of society and the economy. In Pakistan, the increasing reliance on digital systems has made such infrastructure more vulnerable to cyber threats. Recognizing this risk, the Prevention of Electronic Crimes Act, 2016 provides strong legal protections against unauthorized access, data theft, interference, and cyber terrorism related to critical infrastructure. These legal measures play a crucial role in safeguarding national security, maintaining public order, and ensuring the continuous operation of essential services in the country.

Cyber Laws

Q.	Define and distinguish between Integrity, confidentiality, and availability of data in the context of cyber security. **(Imp)**

Ans:

Introduction

In today's digital age, data is the backbone of communication, business, governance, and personal life. Every activity—from online banking to social media—depends on the secure handling of information. With the rapid growth of technology, the risks associated with data misuse, cyber attacks, and unauthorized access have also increased significantly. To address these risks, cyber security introduces three fundamental principles known as Confidentiality, Integrity, and Availability (CIA Triad). These principles ensure that data is protected from unauthorized access, remains accurate and reliable, and is available when needed. In Pakistan, these concepts are also reflected in the legal framework, especially under the Prevention of Electronic Crimes Act (PECA), 2016, which aims to protect information systems and users from cyber threats.

Concept of CIA Triad in Cyber Security

The CIA Triad is a basic model used in cyber security to guide policies, practices, and legal protections related to information systems. It provides a clear understanding of how data should be protected in any digital environment.

These three principles are interrelated, and failure in one can affect the others. For example, if a system is not available, even secure and accurate data becomes useless. Similarly, if confidentiality is breached, sensitive information may be misused even if it remains accurate and accessible.

- **Confidentiality** protects secrecy and privacy of data.
- **Integrity** ensures correctness and trustworthiness of data.
- **Availability** guarantees access to data when required.

Together, they form a complete framework for protecting digital information.

Integrity of Data

Integrity refers to the protection of data from unauthorized alteration, deletion, or modification. It ensures that data remains accurate, consistent, and reliable throughout its lifecycle. In legal and technical terms, integrity is essential because decisions, transactions, and records depend on correct data.

Integrity is not only about preventing changes but also about ensuring that any authorized changes are properly recorded and verified.

Key Aspects of Integrity

Integrity plays a crucial role in maintaining trust in digital systems, especially in sectors like banking, healthcare, and government.

- **Protection from Unauthorized Modification**
  Data must not be altered by unauthorized individuals.
  For example, if a hacker changes examination results in a university database, it directly affects students' careers and violates integrity.

- **Accuracy and Reliability of Data**
  Data must always reflect the true and correct information.
  For instance, in a banking system, the amount of money in an account must always be accurate after each transaction.

- **Consistency of Data Over Time**
  Data should remain consistent unless properly updated.
  For example, if a company's financial records change without proper authorization, it creates confusion and legal issues.

- **Use of Security Mechanisms**
  Tools like hashing, checksums, and digital signatures are used to ensure that data has not been altered. These tools help detect even small changes in data.

Examples of Integrity Violation

- A cybercriminal changes land ownership records in a government database.
- An employee modifies company data to hide fraud.
- Malware alters files in a computer system without the user's knowledge.

Legal Perspective in Pakistan

Under PECA 2016, integrity is protected through provisions such as:

- **Section 5 (Interference with information system or data)**, which criminalizes unauthorized alteration or damage to data.

- **Sections 6–8**, which deal with interference in critical infrastructure systems, showing the importance of maintaining integrity in sensitive sectors like energy and defense.

Confidentiality of Data

Confidentiality means ensuring that data is accessible only to authorized individuals and is protected from unauthorized disclosure. It is closely related to the concept of privacy and is essential for maintaining trust between individuals and organizations.

Confidentiality is especially important for sensitive information such as personal data, financial records, medical information, and national security data.

For Complete PDF Please send Rs. 2000/- at following

JAZZ CASH

or

EASYPAISA

and share screenshot via whatsapp:

03213614222