JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 Print ISSN: 3006-5860
DOI: https://doi.org/10.63468/jpsa.4.2.16
Vol. 4 No. 2 (2026)
https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

Cyber Crimes and Security Challenges in Pakistan

Shabana Kausar•
Lecturer at Institute of Law University of Sindh Jamshoro.

Ali Raza Laghari
Assistant Professor at Institute of law University of Sindh Jamshoro.

Muhammad Nouman Jatoi
Civil Judge and Judicial Magistrate MTMC III Tando Allah Yar Sindh.

•Corresponding Author

ABSTRACT

The main objective of present research is to identify all chellenges faced by citizens and law enforcement agencies to cobat cyber security issues and proposed implementable solution. The duality of technology's modernization has both pluses and minuses, including the ramifications caused by modern-day cybercrime. With the implementation of the Prevention of Electronic Crimes Act (PECA) in 2016, Pakistan began to experience an increase in its recognition of cybercrime. The massive growth of internet users creates an ever-expanding risk of being susceptible to cyber threat attacks - whether they be from within or outside of the country. Cybercrime threats in Pakistan consist of identity theft, hacking, online abuse, online fraud, and technology-related financial crimes. To eliminate and limits the impact of cybercrime on Pakistani citizens, law enforcement and the government must assess the environment for cyber threats; identifying these threats in order to take corrective actions but also bolstering their capabilities for responding, strengthening the country's [infrastructure] to deal with incidents that occur, and increasing the general population's awareness of cyber risks and the need to take precautionary measures. Increasing public awareness through education about cybercrime is paramount to limit the proliferation of cybercrime as well as clarifying legislation and policies that protect against cybercrime, improving the capabilities of those involved with protecting against cybercrime, and increasing the effectiveness of existing legislation and policies, and identifying solutions or tools (e.g., legislation/policies) to assist police/complement/integrate with current

resources available for use in combating cybercrime. Research opportunities identified were to analyze the effects of cybercrime on Pakistan's national security, evaluate current legislation and policies and how effective they are, and develop guidelines for identifying and limiting cybercrime. In addition to developing the guidelines for identifying and eliminating cybercrime, exploring how the use of Artificial Intelligence could[be useful for combating cybercrime in Pakistan and] assist Pakistan in developing a national comprehensive strategy to secure and protect its citizens; while utilizing AI-implemented computer software for automatic detection and collection of evidence.
Keywords: Cybercrime, Cybersecurity, Law Making, Threat To Pakistan, Propaganda, Social Engineering

INTRODUCTION

CYBERCRIME:

Cybercrime, an insidious and pervasive form of criminal activity, has evolved in responce with the rapid advancements in technology, posing unprecedented challenges to individuals, organizations, and nations alike. Characterised as computer-generated crimes involving the use of computers and network devices, cybercrimes encompass a wide range of illicit activities perpetrated through modern telecommunication networks, such as the Internet and mobile phones (Donn B. Parker). These offenses are characterized by a criminal motive to intentionally harm the reputation, cause physical or emotional harm, or inflict financial loss upon individuals or groups of individuals directly or indirectly. Time to time given definition of cyber crime by different experts are as following:

Period	Term Used	Key Figure/Entity	Definition Focus
1970s	**Computer Abuse**	Donn B. Parker	Any intentional act involving a computer where a victim suffered a loss and a perpetrator made a gain.
1976	**Computer Crime**	Donn B. Parker	Defined in his seminal book *Crime by Computer* as crimes where the computer is the **object**, **subject**, **instrument**, or **symbol** of the act.
1979	**Legal Definition**	U.S. Federal Proposal	The first proposed federal legislation (Federal Computer Systems Protection Act) defined it as "knowing, willful manipulation" of federal or financial

Period	Term Used	Key Figure/Entity	Definition Focus
			computer systems.
2001	**Cybercrime**	Budapest Convention	The first international treaty to define cybercrime legally, focusing on offenses against the **confidentiality, integrity, and availability** of computer data and systems.

Cybercrimes have far-reaching ramifications beyond what is attributable only to the internet, endangering (or negatively impacting) a person's/human race's security, finances, and welfare as well as that of the country/nation of the world as a whole. The issues associated with cyber crime are garnering more and more attention and examining, particularly with regard to those instances resulting in the wrongful infliction of injury on a victim; and most recent reporting/studies on the data and/or the things that continues to occur with respect to the Cyber space has seen the alarming growth and prevalence of cyber crime is listed among the most serious and pressing threats facing the globe today, in addition to all of the crimes of asset theft (i.e., burglaries), fraud and corruptions. There is no limitation to the locations or areas where cyber crime can occur; it is an international phenomenon that transcends borders and barriers (jurisdictional and otherwise). Cyber crime has also continued to emerge in Pakistan, as has taken place in many countries around the world; and therefore there is a compelling need to continue to create stronger Cyber security measures; more effective Legislative frameworks; and greater collaborative efforts to succeed in combating cyber crime at all levels of society. The cyber crimes committed have increasingly more serious implications on international security as organized criminals increasingly become more sophisticated with their approach to exploiting technological advancements to further their illegal enterprises and/or the conduct of malicious acts. The extent of the anonymity provided to individuals who use the Internet to commit criminal acts allows these individuals the opportunity to commit a variety of crimes, including but not limited to: data theft, identity theft, hacking; espionage; creating new viruses; transmitting pornography via the Internet; committing cyberspace stalking; and committing cyberspace thefts, all while committing their crimes and avoiding being detected, as should have been done by NCCI (National Cyber Crime Agency).

CURENT STRATEGIES FOR 2025-2026

Challenge Category	Reference / Authority	Key Point
Institutional Shift	NCCIA (Est. 2024/25)	Transition from FIA to NCCIA has caused temporary procedural delays in pending cases.
Telecom Security	PTA Annual Report 25	Focuses on the **CTDISR-2025** (Critical Telecom Data and Infrastructure Security Regulations).
Digital Evidence	Qanun-e-Shahadat Order	Article 164 is increasingly under scrutiny for how it treats "automated" or "AI-generated" evidence.
Cyber Warfare	National Security Policy	Addresses "Hybrid Warfare" and the state's approach to disinformation.

The presence of sophisticated Internet systems and digital technology has provided cybercriminals an opportunity to exploit weaknesses, acquire sensitive information, and commit fraud at levels never before experienced (PLD 2002Lah 159). The unprecedented levels of fraud and cybercrime seen in the past few years must develop more sophisticated approaches to the challenges, create stronger cybersecurity infrastructure, and establish countries working together to protect the integrity of cyberspace while protecting the rights and freedoms of all citizens. In summary, the threats to the rights of individuals, organizations, and countries from cybercrime have been significant in this new digital era. All forms of cybercrime are continuing to grow at an alarming rate, and the coordinated effort, the innovative resolve of nations, and the collaborative approach are necessary to discover the root causes, reduce risk, and create a secure, resilient, and trustworthy digital environment for everyone involved. Nations must work together to combat cybercrime and protect the integrity of cyberspace and the rights and freedoms of their citizens. Pakistan has been affected by hybrid warfare to an extent that is out of proportion to its size or population, because it is located in a very dangerous and important area. The combination of local politics, regional politics, and global competition for power has increased the risk to the country and its citizens.

Cybersecurity:

Cybersecurity represents a comprehensive set of techniques, technologies, and methods for protecting systems connected to the internet from various types of cyber threats, vulnerabilities, and attacks (including hardware, software, networks, and data). It is a key component to safeguarding individuals, organizations,

governments, and critical infrastructure from unauthorized access, data breaches, cyberattacks and other malicious acts that could affect the integrity, confidentiality and the availability of resources and information. The following are several organizations and other entities that have provided definitions for cybersecurity that illustrate its multifaceted nature and importance in protecting the cyberspace and digital ecosystems (PLD 2010 SC 265).

International Organization for Standardization (ISO):

Defines cybersecurity or cyberspace security as the preservation of confidentiality, integrity, and availability of information in the cyberspace, emphasizing the importance of maintaining the security and reliability of digital information and resources to support secure and trustworthy digital interactions and transactions (Electronic Transaction Ordinance 2002).

Committee on National Security Systems (CNSS):

Defines cybersecurity as the ability to protect or defend an enterprise's use of cyberspace from an attack conducted via cyberspace, focusing on the proactive and reactive measures to prevent, detect, and mitigate Cybersecurity represents a comprehensive set of techniques, technologies, and methods for protecting systems connected to the internet from various types of cyber threats, vulnerabilities, and attacks (including hardware, software, networks, and data). It is a key component to safeguarding individuals, organizations, governments, and critical infrastructure from unauthorized access, data breaches, cyberattacks and other malicious acts that could affect the integrity, confidentiality and the availability of resources and information. The following are several organizations and other entities that have provided definitions for cybersecurity that illustrate its multifaceted nature and importance in protecting the cyberspace and digital ecosystems (PLD 2010 SC 265). Examples of some of the most commonly cited definitions are given below:

cyber threats and attacks that aim to disrupt, disable, destroy, or maliciously control computing environments and infrastructure, or compromise the integrity and confidentiality of data and information.

National Institute of Standards and Technology (NIST):

Defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks, emphasizing the iterative and dynamic nature of cybersecurity practices, strategies, and solutions that evolve in response to emerging threats, vulnerabilities, and technological advancements, 2024 P Cr. L J 1462 (Muhammad Haseeb Vs. The State) it discusses the standards for digital forensics and the necessity of maintaining a "chain of custody" for electronic data to be admissible in trial.

Core Principles and Components:

Cybersecurity is anchored on several core principles and components that guide the development, implementation, and management of cybersecurity strategies, policies, and practices. These principles include:

Confidentiality and accuracy:

Ensuring that sensitive data and information are accessible only to authorized individuals, entities, or systems, thereby preventing unauthorized access, disclosure, or exposure of sensitive and confidential information. Maintaining the accuracy, consistency, and trustworthiness of data, information, and systems through measures that prevent unauthorized modification, alteration, or tampering of data and resources.

Availability and Resilience: Ensuring timely and reliable access to information, resources, and services by implementing robust and resilient infrastructure, networks, and systems that can withstand and recover from cyber-attacks, disruptions, or failures. Resilience is building and maintaining adaptive, agile, and responsive cybersecurity capabilities that enable organizations to anticipate, withstand, recover from, and adapt to cyber threats, incidents, and challenges.

Genesis of Cybercrime in Pakistan:

The genesis of cybercrime in Pakistan is closely linked with the rapid growth of information and communication technologies and the increasing penetration of the internet in society. In the early stages of digital adoption, cyber-related offenses were limited in scope and primarily involved unauthorized access to computer systems, email misuse, and basic online fraud. Due to limited digital literacy and the absence of comprehensive cyber laws, such offenses often went unreported or were inadequately addressed. As internet usage expanded in the early 2000s, the digital space began to be exploited for criminal activities. The emergence of social media platforms, online banking, and e-commerce created new opportunities for cyber offenders. Crimes such as identity theft, online harassment, defamation, and electronic fraud started to surface, highlighting the darker side of digital advancement. The lack of awareness, weak regulatory mechanisms, and insufficient enforcement infrastructure contributed significantly to the early growth of cybercrime in Pakistan.

The initial response of the state was reactive rather than preventive. Legal frameworks were either outdated or non-existent, leading to challenges in investigation, prosecution, and conviction. This period marked the foundational stage of cybercrime in Pakistan, where technological progress outpaced legal and institutional readiness.

Evolution of Cybercrime in Pakistan:

With the rapid digitalization of society, cybercrime in Pakistan has evolved in both complexity and scale. The evolution of cybercrime can be analyzed through the following key developments. Cybercrime has expanded from simple hacking and email fraud to sophisticated crimes such as phishing, ransomware attacks, financial fraud, cyberstalking, online blackmail, and data breaches. The widespread use of social networking platforms has led to a rise in cyber harassment, hate speech, defamation, fake profiles, and non-consensual sharing of private content, disproportionately affecting women and minors. The digital banking and online payment systems have introduced risks such as online scams, ATM skimming, mobile banking fraud, and cryptocurrency-related crimes and threats.

Cyber Harassment and Online Abuse:

One of the most prevalent forms of cybercrime in Pakistan is cyber harassment, including online stalking, threats, blackmail, and defamation. Social media platforms are frequently misused to target individuals, particularly women, journalists, activists, and public figures. The misuse of images, fake profiles, and non-consensual sharing of private content has caused severe psychological, social, and reputational harm to victims.

Financial Cybercrime:

With the rise of digital banking and online transactions, financial cybercrime has increased significantly. Common offenses include phishing scams, fraudulent calls, fake investment schemes, ATM skimming, and unauthorized access to bank accounts. These crimes not only affect individuals but also undermine trust in digital financial systems, slowing economic digitalization.

Identity Theft and Data Breaches:

Cybercriminals often steal personal data such as CNIC numbers, phone records, and login credentials. This stolen data is used for impersonation, financial fraud, and illegal activities. Data breaches involving both public and private institutions highlight weaknesses in data protection and cybersecurity governance.

Cyberterrorism and State Security Threats:

Cybercrime also poses risks to national security. Cyberterrorism, online radicalization, misinformation campaigns, and attacks on critical digital infrastructure represent emerging threats. These activities exploit cyberspace to destabilize social order and spread fear without physical violence.

Causes Behind the Growth of Cybercrime:

The rise of cybercrime in Pakistan is driven by multiple interconnected factors. The rapid pace of technological adoption has outstripped legal and institutional preparedness. Laws, enforcement agencies, and judicial mechanisms have struggled to keep pace with evolving cyber threats.

Lack of digital literacy and public awareness significantly contributes to victimization. Many users unknowingly share personal information, fall for online scams, or fail to secure their digital devices. Weak enforcement mechanisms and low conviction rates reduce deterrence, allowing cybercriminals to exploit jurisdictional gaps, anonymity, and technical complexity. Socio-economic pressures such as unemployment and limited regulatory oversight have also pushed some individuals toward cybercrime as an alternative means of income.

Organized and Transnational Nature:

Cybercrime has evolved from individual offenders to organized criminal networks operating across borders, making detection and prosecution more challenging. akistan introduced the Prevention of Electronic Crimes Act (PECA) 2016 to address emerging cyber threats. Specialized cybercrime wings and digital forensic units have been established to investigate and prosecute cyber offenses. Cybercriminals now employ advanced tools such as malware, spyware, social

engineering techniques, and artificial intelligence to exploit vulnerabilities in digital systems.

Challenges in Enforcement and Awareness:

Despite legal advancements, enforcement remains limited due to resource constraints, lack of technical expertise, jurisdictional issues, and low public awareness. The genesis and evolution of cybercrime in Pakistan reflect the unintended consequences of rapid digital transformation. While digital technologies have brought significant social and economic benefits, they have also created new avenues for criminal exploitation. Cybercrime in Pakistan has evolved from isolated and simple offenses to complex, organized, and technologically advanced crimes. Addressing this dark side of the digital age requires not only robust legal frameworks and effective enforcement mechanisms but also public awareness, digital literacy, and continuous adaptation to emerging technological threats.

Digital Transformation and Vulnerability in Pakistan:

Pakistan has witnessed significant growth in internet usage, mobile connectivity, and digital platforms over the past decade. Increased access to smartphones, social media, online banking, and e-commerce has reshaped daily life. However, this rapid digital transformation has occurred in a context marked by limited cybersecurity awareness, weak digital literacy, and socio-economic disparities.

These factors have created vulnerabilities that cybercriminals exploit. Many users lack knowledge about data privacy, secure online behavior, and cyber risks, making them easy targets for fraud, harassment, and exploitation. The absence of strong cybersecurity infrastructure at both individual and institutional levels further amplifies exposure to cyber

Legal Framework Governing Cybercrime in Pakistan :

Pakistan's primary cybercrime legislation is the Prevention of Electronic Crimes Act 2016, which criminalizes offenses such as unauthorized access, cyber terrorism, electronic fraud, cyberstalking, and hate speech. While this law represents a significant legislative step, it faces criticism for vague definitions, potential misuse, and inconsistent enforcement.

Procedural delays, lack of trained investigators, and limited forensic capacity hinder effective implementation. Additionally, cybercrime cases often involve cross-border elements, complicating investigation and prosecution due to jurisdictional limitations and weak international cooperation mechanisms. 2024 P Cr. L J 1462 (Muhammad Haseeb Vs. The State), Discusses the standards for digital forensics and the necessity of maintaining a "chain of custody" for electronic data to be admissible in trial.

Institutional Response and Challenges :

The Federal Investigation Agency Cyber Crime Wing is the primary body responsible for investigating cyber offenses in Pakistan. Despite its mandate, the agency faces challenges including limited resources, heavy caseloads, technical constraints, and public mistrust.

Victims often hesitate to report cybercrime due to fear of stigma, lengthy procedures, and lack of confidence in outcomes. This underreporting distorts the true scale of cybercrime and weakens policy responses. Judicial handling of cybercrime cases also presents challenges, as courts may lack technical expertise, leading to delays and difficulties in evaluating digital evidence.

Social and Psychological Impact of Cybercrime:

Cybercrime has profound social and psychological consequences. Victims frequently experience anxiety, depression, social isolation, and reputational damage. In conservative social settings, online harassment can result in severe social repercussions, particularly for women.

At a broader level, cybercrime erodes public trust in digital platforms and institutions, discouraging digital participation and innovation. This undermines national objectives related to digital economy development and e-governance.

Critical Analysis of the Dark Side of the Digital Age:

The digital age, while offering unprecedented connectivity and efficiency, has also blurred boundaries between public and private life. Technologies that empower individuals can be weaponized for surveillance, manipulation, and exploitation.

Cybercrime in Pakistan illustrates how technological progress without parallel ethical, legal, and educational development creates systemic risks. The digital divide, weak governance, and social inequalities further intensify these risks, making cybercrime not merely a technological issue but a broader socio-legal problem.

Relevent Case Laws in Pakistan:

Judicial interpretation has played a critical role in shaping the understanding and enforcement of cybercrime laws in Pakistan. The courts have not only addressed criminal liability arising from digital offenses but have also examined the constitutional implications of cyber regulation. The following five cases illustrate how Pakistani courts have dealt with various dimensions of cybercrime.

In Shehzad v. State (2023 SCMR 679), the Supreme Court of Pakistan examined allegations involving cyber harassment and unauthorized access under the Prevention of Electronic Crimes Act 2016 alongside provisions of the Pakistan Penal Code. The Court emphasized that electronic evidence must be collected and evaluated with strict adherence to legal standards. It held that vague allegations without reliable digital proof cannot justify prolonged detention, thereby reinforcing the importance of due process in cybercrime prosecutions.

In the case of Pakistan Federal Union of Journalists v. Federation of Pakistan (Islamabad High Court, 2022), the Court struck down amendments introduced through the Prevention of Electronic Crimes Ordinance 2022. The Court held that provisions criminalizing online defamation and false information were vague and disproportionate, violating constitutional guarantees of freedom of expression,

privacy, and due process. This case highlighted the judiciary's role in preventing the misuse of cybercrime laws as tools of censorship.

In Imran Khan v. Federation of Pakistan (Islamabad High Court, 2023) examined the application of PECA provisions concerning online speech and political expression. The Court emphasized that criticism of public officials on digital platforms, unless falling within clearly defined legal limits, remains protected under the Constitution. The judgment reinforced that cyber laws must be interpreted narrowly to avoid suppressing legitimate democratic discourse.

In Ali Raza v. State (Lahore High Court, 2021), the Court addressed the issue of cyber harassment and blackmail involving social media platforms. The Court upheld the applicability of PECA provisions while stressing the need for prompt investigation and victim protection. It recognized the serious psychological and social harm caused by online harassment, particularly in cases involving non-consensual sharing of private content.

In Muhammad Aslam v. FIA (Peshawar High Court, 2020), the Court examined procedural irregularities in cybercrime investigations conducted by enforcement agencies. The Court suspended enforcement action due to non-compliance with statutory safeguards, emphasizing that investigative powers under PECA must be exercised lawfully and transparently. This case underscored judicial concern over arbitrary use of cybercrime laws.

These five cases collectively demonstrate that Pakistani courts seek to balance effective cybercrime control with the protection of constitutional rights. Judicial oversight remains a key mechanism in addressing the dark side of the digital age.

Interview Transcripts on the Dark side of Cybercrime in Pakistan:

This annexure presents interview responses collected for the qualitative analysis of cybercrime as the dark side of the digital age in Pakistan. The interviews were conducted to gather informed perspectives from individuals professionally connected to law, technology, media, and digital governance.

Respondent no. 1: Name Ahmed Raza Profession Advocate

Question: What are the trends and patterns of cybercrime in Pakistan?

Response: Cybercrime in Pakistan is increasingly sophisticated, with patterns ranging from online harassment, fraud, and identity theft to cyberterrorism. Organized cybercriminal activities exploit social media and digital financial platforms. Legal enforcement struggles to keep pace with these evolving threats.

Respondent no. 2: Name Sara Khan Profession Digital Rights Activist

Question Most common type of cybercrime in Pakistan?

Response: Online harassment and financial fraud are the most common types. Young people and women are particularly vulnerable, and social media platforms are often used to carry out these offenses.

Respondent no.3: Name Muhammad Usman Profession Information Technology Specialist

Question How does cybercrime affect national security and individuals in Pakistan?

Response: Cybercrime poses risks to national security by targeting critical infrastructure and spreading misinformation. For individuals, it results in financial loss, identity theft, and emotional stress.

Respondent no. **4:** Name Farah Siddiqui Profession : Journalist

Question: How can Pakistan enhance its cybersecurity?

Response: Strengthening laws, investing in technical infrastructure, training enforcement personnel, and conducting public awareness campaigns are essential. Protection for journalists and activists online is also critical.

Respondent no. 5: Name Ayesha Memon Profession: Social Worker

Question: What are the challenges in investigations of cybercrime?

Response: Investigations face challenges such as lack of trained personnel, limited forensic resources, procedural delays, and cross-border jurisdiction issues. Victims often hesitate to report crimes due to social stigma and fear.

DISCUSSION

The interviews provide a concise yet comprehensive understanding of cybercrime in Pakistan. Legal professionals, activists, IT specialists, journalists, and social workers highlighted key issues: the prevalence of online harassment and fraud, risks to national security, weaknesses in law enforcement, and social and psychological consequences for victims. These perspectives underscore that cybercrime is not only a legal and technical problem but also a societal challenge that requires coordinated action across multiple sectors. Strengthening legislation, improving enforcement, enhancing digital literacy, and promoting public awareness are essential to effectively mitigate cybercrime in Pakistan. The insights from these interviews complement the findings in Chapter 5 and provide practical guidance for policy and strategic interventions.

History of cybersecurity problems: In Pakistan, cybercrime was not of a serious concern of the state at early decades, at that time there was no awareness in society too. There was no special law with regards to the cybercrime but with the passage of time as increasing rate in cybercrimes in Pakistan, compelled the legislature to make laws regarding it. The very first legislation that Pakistan has in place is 'Electronic Transactions Ordinance, 2002' which deals with cybercrime issues.

This ordinance was enacted by the President of Pakistan with the aim of 'recognizing and facilitating documents, records, information, communications and transactions in electronic form, there was no recognition for electronic documents before the passing of ETO.

Cybercrime was also recognized in ETO wherein unauthorized access and damage to information system were made punishable under the law. However, that did not address the entire cybercrime scenario and not much was covered by this law. For the second time another considerable legislation in the Pakistani legal system, "Prevention of Electronic Crimes Ordinance, 2007" was enacted to raise public awareness of electronic crimes.

Thereafter in 2014 a "National Action Plan" was implemented in the country, consisting of 20 action items to be implemented to counter extremism. In

February 2015, a draft bill was approved to be introduced in the Parliament. The bill was approved by the National Assembly in April 2016. The Senate unanimously passed the bill in July 2016 with 50 amendments to the original draft and was named as Prevention of Electronic Crimes Act, 2016. PECA, 2016 ensures hacking, digital piracy, cyberbullying, cyberstalking, identity theft, doctoring images and spoofing as serious punishable offences. As PECA,

2016 called complete legislation ensures electronic fraud, forgery, unauthorized access into an information system as serious offences under this Act. By the implementation of this ACT it also grants punishment for Whereas, on the other hand when we get to know about the laws related to the defense of 5thgeneration war, there is none till date. Which means that Pakistan is in a battlefield without its armor to protect itself and in addition to that its people are not even aware that their country is in the battled and in the last addition to it that they are even unaware that they sometimes are being used against their own homeland and how is that is shared in the subsequent writing.

The Legal Framework and Its Limitations

The foundational principle of criminal law is predicated on the premise that for an act to be deemed criminal and punishable there must be a corresponding law that defines, proscribes, and penalizes the act. This principle, rooted in the rule of law and the protection of individual rights and liberties, ensures that individuals are aware of their obligations, responsibilities, and the consequences of their actions, thereby fostering a just, equitable, and accountable society. However, the emergence of cybercrimes, hybrid warfare, and unconventional threats has exposed gaps, inadequacies, and limitations in existing legal frameworks, particularly in addressing the complexities and nuances of modern warfare, conflict, and crime in cyberspace and digital domains. Following laws are presently active and addressing threats of cyber world:

· **Cyber Crime Investigation Agency (NCCIA)**, replacing the FIA's NR3C as the lead investigative body. It also introduced tougher penalties for digital defamation and "aspersions" against state institutions.

· **Electronic Transactions Ordinance (ETO), 2002:** Still relevant for the legal recognition of digital signatures and electronic documents.

· **Removal and Blocking of Unlawful Online Content Rules, 2021:** Governs how the PTA handles social media content. 2018 YLR 329 (Farhan Kamrani Vs. The State): A landmark case regarding cyberstalking and the dignity of a natural person. It set a precedent for how social media evidence (screenshots and URLs) must be verified by the FIA/investigating agencies.

On Jurisdictional Overlap: Muhammad Ayyaz Bin Tariq Vs. Federation (2024): The Islamabad High Court clarified the jurisdiction of special courts under PECA. It addressed whether offenses under the Pakistan Penal Code (PPC) can be tried alongside PECA offenses in the same specialized forum. Crl. Bail Application No. S-

357 of 2025 (Sindh High Court): A recent ruling clarifying that while certain cyber-crimes (like Section 21 - modesty of a person) are listed in the Anti-Rape Act, they are still primarily triable by PECA-designated courts unless actual sexual assault is involved.

On Freedom of Speech vs. Regulation: The "Mehram Ali" Case Principle: Frequently cited in 2025/2026 challenges against the new Social Media Protection Tribunals. This principle dictates that all judicial/quasi-judicial tribunals must remain under the supervision of High Courts to ensure independence from the executive branch.

The imperative of lawmaking in addressing emerging threats, such as cybercrimes and hybrid warfare, cannot be overstated, as it represents a proactive, strategic, and comprehensive approach to mitigating risks, enhancing resilience, and preserving national security and stability. The development and implementation of robust, adaptive, and forward-looking legal frameworks are essential to:

Define and Proscribe Cybercrimes: Establish clear, precise, and comprehensive definitions and provisions that criminalize a broad range of cyber activities, including unauthorized access, data breaches, cyber-attacks, information warfare, and other malicious activities that pose threats to individuals, organizations, and critical infrastructure.

Regulate and Govern Cyber Operations: Develop regulatory frameworks and governance mechanisms to oversee and manage cyber operations, activities, and initiatives, ensuring compliance with international laws, norms, and standards, and promoting responsible behavior in cyberspace. Recognize, define, and address hybrid threats and warfare strategies that combine conventional, irregular, and cyber warfare tactics, methodologies, and techniques to achieve strategic objectives and influence outcomes in the digital domain.

Need of International Cooperation and Collaboration: Foster collaboration, information sharing, and coordination among nations, governments, and international organizations to address common challenges, share best practices, and promote collective security and stability in cyberspace and digital ecosystems.

By strengthening legal mechanisms, capabilities, and capacities to protect and safeguard national security, sovereignty, and critical infrastructure from cyber threats, hybrid warfare, and external interference, ensuring the integrity, resilience, and reliability of national systems, networks, and resources. The imperative of lawmaking in addressing contemporary threats, such as cybercrimes and hybrid warfare, is essential to fostering a secure, resilient, and trustworthy digital environment that supports innovation, collaboration, and prosperity in the digital age. By developing and implementing robust, adaptive, and comprehensive legal frameworks, nations, governments, and international organizations can effectively mitigate risks, address vulnerabilities, and shape a secure, stable, and prosperous future for all in an interconnected and contested global landscape.

1. **Global Treaty Participation**:

UN Convention Against Cybercrime: Pakistan has been an active participant in the UN Ad Hoc Committee. Following the adoption of the UN Convention against

Cybercrime in late 2024, Pakistan has moved toward alignment with this global framework, which facilitates the sharing of electronic evidence for serious crimes across borders.

The Budapest Convention Debate: While Pakistan traditionally hesitated to join the Budapest Convention (Council of Europe), by 2025/2026, the Ministry of IT (MoITT) and the Interior Ministry have been in advanced consultations to finalize a viewpoint on accession or a similar Mutual Legal Assistance Treaty (MLAT) with the US. This is specifically aimed at gaining faster access to data held by tech giants like Google, Meta, and X (Twitter).

2. **Institutional Collaboration**:

Establishment of NCCIA (2025): The National Cyber Crime Investigation Agency (NCCIA) was established with a specific mandate to act as the central point for international cooperation. Under the PECA Amendment Act 2025, the NCCIA is empowered to engage directly with international agencies (like INTERPOL) for the extradition of cybercriminals and the retrieval of overseas data.

PKCERT (National CERT): Pakistan's National Computer Emergency Response Team (PKCERT) now collaborates with international CERTs. In 2024, it was recognized for its progress in "Global Cooperation "one of the five pillars of the ITU Index specifically for its threat-intelligence sharing protocols.

3. **Bilateral & Regional Strategic Partnerships**:

Strategic Partnerships (e.g., Kazakhstan 2026): Just recently, in February 2026, Pakistan and Kazakhstan signed a joint declaration to establish a High-Level Security Dialogue, which includes specific working groups on IT, telecommunications, and digital asset regulation.

DCO (Digital Cooperation Organization): Pakistan is a founding member of the DCO. It uses this platform to harmonize digital tax and cybersecurity policies with other member states (including Saudi Arabia and the UAE) to create a "unified cyber-defense" front in the Global South.

Capacity Building Programs: Programs like the IELP (International Exchange and Leadership Program) with the U.S. have trained Pakistani law enforcement in digital forensics and cross-border enforcement, specifically focusing on the Department of Justice's standards for evidence.

ANTECEDANT STATE ACTIONS: In addition to the above cited enactments and working of the ruling governments as given in the background, as per the Express Tribune report: "The government gave a go-ahead to a National Cyber Security Policy 2021, under which a national cybersecurity response framework will be created. To ensure proper implementation of the policy, a Cyber Governance Policy Committee has been formed. The policy is set to introduce strict action against cyber-attacks targeting any state institution, terming it as an "act of aggression against national sovereignty". It will also focus on countering the different types of incidents that involve misuse of the information and other related communication technologies that could put financial matters in disarray. Under the said policy, the Cybercrime Wing of the Federal Investigation Agency (FIA) has been tasked to

introduce a Cyber Patrolling Unit (CPU) to keep a check on what is trending on the internet." As such actions accrue not only anti-government policy but are somehow being played in the external hands by forming negative propagandas against the state. The report further states: "At present, the main law for cyber security in the country is Prevention of Electronic Crime Act (PECA) meant to prevent and detect offences relating to the cyber world. PECA was introduced in 2016. It provides a comprehensive framework for various types of cybercrimes in Pakistan which, in sync with the Cyber Crime Bill 2007, deals with internet crimes in the country, such as illegal access to data (through hacking), Denial of Service Attacks (DOS Attack), electronic forgery and electronic fraud, and cyber terrorism. The main intent and purpose behind the enactment of the Act are to create deterrence against the misuse of cyberspace and to criminalize and punish certain acts and offences. The penalties awarded on proof of offence are: up to three years of imprisonment, Rs1 million fine, or both for accessing critical information systems without authorization; up to seven years of imprisonment, Rs10 million fine or both for disruption of critical information systems with dishonest or fraudulent intentions; up to seven years of imprisonment, Rs10 million fine or both for involvement in offence related to terrorism; up to six months of imprisonment, Rs50 thousand fine or both for importing, exporting or supplying an electronic device for offensive use; and up to three years of imprisonment, Rs5 million fine or both for involvement in a data breach" as to penalize and prevent the criminal intent behind such actions.

THE FOREGOING INSTITUTIONAL WORKING:

According to the report of the Express Tribune Newspaper: "In pursuance of the PECA Act, detailed rules now provide procedures for the proper functioning of the investigative agency designated therein. FIA will have Cyber Crime Wings, which include the investigation and forensic section. To detect and prevent cybercrimes, data and networks have been designated, which will also enable the aggrieved to seek the remedy from there. They also have the option of suing for damages. The FIA claims to have established, cybercrime help desk, cybercrime reporting centers and complaint management units at cyberheadquarters and all cybercrime reporting centers with an objective to provide easy access to the complainant. These centers have been tasked to digitalize registration and expedite the processing of cybercrime complaints.

Although considerable initiative for cyber security through the implementation of laws has been taken, there is a lot more that needs to be done. Under the PECA 2016, the federal government has gained the authority to designate any agency to take cognizance of cybercrime, but only FIA has been empowered to do so, ignoring the police within the province. However, FIA suffers from human resource problems and is confined to specific areas in major cities. Therefore, it is out of reach for the general population. In contrast to this, police stations are available in every nook and corner and easily accessible to all and sundry." So that is to say that further rule making is required so as to make such working provided for the masses and to the every corner of the country because the FIA lacks in the human resource

and also to the identification of public and the places in the suburbs, either it shall have the power to further designate to the local police or whole of the working be handed over to the local police of such locality and such local police be trained accordingly to the cyber-security, combat its threats, prevention and execution. ____

Internal Challenges in Combating Cybercrime in Pakistan:

Weak Technological Infrastructure: Pakistan faces serious limitations in technological infrastructure required to combat cybercrime effectively. Many investigative agencies lack access to modern digital forensic laboratories, secure data storage systems, and advanced cyber monitoring tools. Cybercriminals employ sophisticated technologies such as encryption, virtual private networks, anonymization tools, and dark web platforms, creating a significant imbalance between offenders and law enforcement authorities.

Lack of Skilled and Trained Human Resources:

Cybercrime investigation requires specialized expertise in information technology, digital forensics, and cybersecurity. Pakistan faces a shortage of trained personnel within law enforcement agencies, prosecution departments, and the judiciary. Limited training opportunities and absence of continuous professional development hinder effective investigation and prosecution of cyber offenses.

Limited Public Awareness and Digital Illiteracy: A substantial portion of the population lacks awareness of cyber threats and safe digital practices. Individuals frequently become victims of phishing, online fraud, identity theft, and cyber harassment due to low digital literacy. Many victims hesitate to report cybercrimes because of fear, lack of trust in institutions, or ignorance of legal remedies.

Weak Enforcement of Cyber Laws: Despite the existence of cybercrime legislation, enforcement remains inconsistent. Investigative delays, procedural inefficiencies, lack of technical understanding, and improper handling of digital evidence weaken the effectiveness of cyber laws and reduce their deterrent impact.

Institutional Coordination Issues: Cybercrime investigations involve multiple agencies including law enforcement bodies, regulatory authorities, financial institutions, and internet service providers. Poor coordination, overlapping responsibilities, and lack of a centralized response mechanism cause delays and reduce the effectiveness of enforcement efforts.

External Challenges in Addressing Cybercrime

Transnational Nature of Cybercrime: Cybercrime transcends national boundaries. Many cyber offenses affecting Pakistan originate from foreign jurisdictions, making investigation and prosecution difficult. Jurisdictional limitations and sovereignty concerns restrict the ability of domestic authorities to take effective action against offenders operating abroad.

Limited International Cooperation: Effective control of cybercrime requires international collaboration, information sharing, and legal assistance. Pakistan faces challenges due to limited international agreements and delays in obtaining digital evidence from foreign service providers and technology companies.

Dependence on Foreign Digital Platforms: Most digital platforms used in Pakistan are owned and operated by foreign companies. Limited regulatory control over these platforms restricts access to user data and weakens enforcement against cyber offenders.

Legal and Regulatory Challenges:

Ambiguities in Cyber Legislation: Certain provisions of cyber laws lack clarity regarding jurisdiction, surveillance, and procedural requirements. These ambiguities create uncertainty in enforcement and result in inconsistent judicial interpretations.

Challenges in Digital Evidence and Admissibility: Digital evidence is highly sensitive and easily altered. Lack of standardized forensic procedures, weak chain of custody, and limited technical understanding often lead to challenges in courts regarding authenticity and reliability of evidence.

Security Challenges in the Digital Age: Threats to National Security and Critical Infrastructure: Cybercrime increasingly targets critical infrastructure including power systems, financial institutions, communication networks, and government databases. Cyberattacks on such systems pose serious threats to national security and public safety.

1.Cyber Espionage and Data Breaches: Unauthorized access to confidential information, data theft, and cyber espionage threaten both state institutions and private organizations. Weak cybersecurity measures increase vulnerability to large scale data breaches and financial losses.

2. Financial Security and Digital Banking Risks: The expansion of digital banking and online financial services has increased exposure to cyber fraud, hacking, and ransomware attacks. Inadequate cybersecurity controls in financial institutions can undermine economic stability.

3. Challenges in the Cyber Domain: Rapid Technological Advancement: Technological developments evolve faster than legal and institutional frameworks. Cybercriminals exploit emerging technologies such as artificial intelligence, cryptocurrencies, and anonymization tools, while enforcement agencies struggle to adapt.

Anonymity and Attribution Difficulties: Cyber offenders often conceal their identities through encrypted communication and anonymous networks. Identifying perpetrators and attributing cyber offenses remains a major challenge in the cyber domain.

Misuse of Social Media and Digital Platforms: Digital platforms are widely used for cyber harassment, blackmail, misinformation, hate speech, and online manipulation. Regulating such misuse while protecting fundamental rights remains a complex challenge.

4. Lack of Cybersecurity **Culture:** Both public and private sectors lack a strong cybersecurity culture. Poor security practices, weak password management, and negligence in data protection increase vulnerability to cyber threats.

5. Socio Economic and Cultural Challenges: Limited financial resources restrict investment in cybersecurity infrastructure, training programs, and awareness campaigns. Cybersecurity often receives lower priority despite its growing importance.

Social Stigma and Underreporting:Victims of cybercrime, particularly cyber harassment, often avoid reporting incidents due to fear of social stigma and reputational harm. This underreporting enables cyber offenders to continue their activities without accountability.

6. Digital Transformation and the Expansion of Cyber Risk**:** The digital revolution has fundamentally reshaped social, economic, and governmental structures in Pakistan. The integration of digital technologies through mobile connectivity, electronic commerce, online financial services, social media platforms, and e-governance systems has created new efficiencies and opportunities. At the same time, rapid digitization has expanded the scope, scale, and complexity of cybercrime, exposing serious weaknesses within Pakistan's legal, institutional, and security frameworks.

7. Institutional Capacity and Enforcement Constraints: Law enforcement agencies face significant institutional limitations in addressing cybercrime. These include outdated technological tools, insufficient digital forensic facilities, weak cyber intelligence mechanisms, and absence of specialized cyber units at provincial and district levels. Such constraints delay investigations and reduce enforcement effectiveness.

8. Human Resource and Skill Deficiencies**:** Cybercrime investigation requires specialized expertise in cybersecurity, digital forensics, and information systems. Pakistan faces a shortage of trained personnel within law enforcement agencies, prosecution services, and the judiciary. Limited training and lack of continuous professional development weaken the ability to investigate and prosecute complex cyber offenses.

9. Public Awareness and Digital Vulnerability: Low levels of digital literacy and cybersecurity awareness contribute to widespread cyber victimization. Individuals frequently engage with digital platforms without understanding privacy risks and online safety practices. Underreporting of cybercrime due to fear, social stigma, and lack of trust in institutions conceals the true magnitude of the problem.

10. Legal Framework and Implementation Challenges: The Prevention of Electronic Crimes Act 2016 provides the primary legal framework for addressing cybercrime in Pakistan. However, ambiguities in legal provisions, jurisdictional challenges, procedural inefficiencies, and difficulties in collecting and admitting digital evidence undermine effective implementation and consistent judicial outcomes.

11. Cybersecurity and National Security Implications: Cybercrime poses serious threats to national security by targeting financial systems, communication networks, government databases, and critical infrastructure. The growing overlap between cybercrime, cyber terrorism, and cyber espionage elevates cybersecurity to a strategic national concern.

Socio-Economic and Cultural Constraints

Limited financial resources restrict investment in cybersecurity infrastructure, capacity building, and public awareness initiatives. Cultural barriers discourage reporting of cyber harassment and exploitation, particularly among women, allowing cybercrime to persist with limited accountability.

Fault Lines: Pakistan's fault lines in cybersecurity include gaps in legal frameworks, weak institutional coordination, insufficient human resources, limited digital literacy, and structural underinvestment in cyber defense. Social and cultural barriers, combined with inconsistent public reporting and low awareness, exacerbate vulnerabilities. Technological fault lines include outdated systems, weak encryption standards, and lack of national-level threat intelligence sharing.

Strengths: Pakistan's emerging strengths include the establishment of specialized cybercrime units, growing investment in digital infrastructure, increasing awareness of cybersecurity issues, and academic programs producing trained professionals. Public-private partnerships and international collaborations offer frameworks for adopting global best practices and improving cyber resilience.

Opportunities: Opportunities exist to strengthen Pakistan's cyber defense through comprehensive legal reform, investment in advanced security technologies, and enhanced public awareness initiatives. Encouraging innovation in cybersecurity startups, developing national threat intelligence frameworks, and promoting regional cooperation for cross-border cybercrime investigation can improve overall resilience. Expanding digital literacy and targeted training programs can also mitigate vulnerabilities and build a sustainable cybersecurity ecosystem.

Strategic Significance of Cybercrime Governance: Effective governance of cybercrime in Pakistan requires coordinated legal reform, institutional strengthening, technological modernization, public awareness, and international cooperation to protect digital trust, economic stability, and national security in the digital age. Leveraging strengths and opportunities while addressing fault lines is essential to transform Pakistan's cyber ecosystem into a secure and resilient environment.

AN ANALYSIS OF THE DARK SIDE OF THE DIGITAL AGE CYBERCRIME IN PAKISTAN:

Qualitative analysis of cybercrime in Pakistan reveals that despite the enactment of the Prevention of Electronic Crimes Act 2016, the social and institutional aftermaths of cyber offenses remain severe. Victim narratives and reported cases indicate that individuals continue to suffer psychological trauma, reputational harm, and social exclusion following cyber harassment, identity theft, online fraud, and blackmail. Although PECA 2016 criminalizes such conduct, qualitative evidence suggests that fear of stigma, lack of confidentiality, and limited awareness of legal rights discourage victims from invoking the law. This gap between statutory protection and lived experience weakens the intended deterrent effect of PECA 2016.

At the institutional level, enforcement under PECA 2016 faces challenges including procedural delays, limited forensic expertise, and inconsistent application

of legal provisions. These shortcomings contribute to public mistrust in the cybercrime justice system and undermine confidence in digital platforms and online governance.

Institutional and Legal Gaps in the Implementation of PECA 2016

Interpretive examination of PECA 2016 highlights several structural limitations in its implementation. While the Act provides investigative powers and penal provisions, qualitative assessment shows ambiguity in certain sections related to jurisdiction, data retention, and content regulation. These ambiguities create enforcement discretion that may lead to inconsistent outcomes and concerns regarding misuse.

Furthermore, limited judicial and investigative training in digital evidence handling affects the effective prosecution of cyber offenses. The absence of a comprehensive data protection regime alongside PECA 2016 also leaves personal information vulnerable, exacerbating cybercrime risks and reducing public trust.

Qualitatively Informed Policy Suggestions within the Framework of PECA 2016

Victim centred reforms should be introduced within the PECA 2016 framework to ensure confidentiality, procedural fairness, and protection against secondary victimization. Establishing clear reporting protocols and support mechanisms would encourage greater public engagement with cybercrime laws.

Capacity building of the Federal Investigation Agency Cyber Crime Wing should be prioritized through specialized training in digital forensics, ethical investigation, and human rights compliance. Such reforms align with the objectives of PECA 2016 by strengthening lawful enforcement while preventing arbitrary application. Digital literacy initiatives should be formally integrated into national cyber policy to complement PECA 2016. Qualitative analysis indicates that legal deterrence alone is insufficient without public understanding of cyber risks, online safety, and legal remedies.

Way Forward for Pakistan in Light of PECA 2016:

Pakistan's cybercrime governance must evolve toward an adaptive and rights based model consistent with PECA 2016 and constitutional guarantees. Periodic legislative review is necessary to address emerging threats such as artificial intelligence driven fraud, deepfake misuse, and cross border cybercrime that were not fully anticipated at the time of enactment.

A socio legal approach should be adopted to ensure that cyber laws function effectively within Pakistan's cultural and social context. Community engagement, civil society participation, and institutional transparency can bridge the gap between law and society.

Independent oversight and judicial scrutiny should be strengthened to ensure that investigative powers under PECA 2016 are exercised proportionately and transparently. This approach will help balance cybersecurity objectives with fundamental rights, including privacy and freedom of expression.

CONCLUSION

Aligning qualitative analysis with PECA 2016 demonstrates that while Pakistan possesses a foundational cybercrime law, its effectiveness depends on implementation, institutional capacity, and public trust. The dark side of the digital age cannot be addressed through legislation alone. A holistic strategy combining legal reform, institutional strengthening, digital literacy, and rights based governance is essential to ensure that PECA 2016 fulfils its purpose in safeguarding Pakistan's digital future. The digital transformation of Pakistan has created unprecedented opportunities for communication, commerce, and governance, but it has also exposed individuals and institutions to complex and evolving forms of cybercrime. The analysis of the dark side of the digital age demonstrates that cybercrime in Pakistan is not merely a technological issue but a multidimensional challenge rooted in legal, social, and institutional weaknesses. While the Prevention of Electronic Crimes Act 2016 provides a foundational legal framework, qualitative assessment reveals that gaps in implementation, limited institutional capacity, and lack of public awareness continue to undermine its effectiveness The persistence of cybercrime highlights the disconnect between law on paper and law in practice. Victim experiences, enforcement limitations, and societal factors such as stigma and digital illiteracy indicate that legal deterrence alone is insufficient. Effective cybercrime governance requires a holistic approach that integrates victim protection, institutional accountability, digital literacy, and rights-based enforcement. Looking ahead, Pakistan's ability to secure its digital future depends on its commitment to adaptive legal reform, professional capacity building, and transparent governance under PECA 2016. By aligning cybersecurity objectives with constitutional safeguards and societal realities, Pakistan can mitigate cyber threats while fostering public trust in digital systems. Addressing the dark side of the digital age is therefore essential not only for legal compliance but for sustainable digital development and the protection of fundamental rights in an increasingly connected society.

Recommendations

Pakistan should strengthen the implementation of the Prevention of Electronic Crimes Act 2016 by removing procedural ambiguities and ensuring uniform application across jurisdictions. Continuous training of law enforcement and judicial officers in digital forensics and cyber law is essential to improve investigation and prosecution outcomes.

Victim protection mechanisms must be enhanced through confidential reporting systems, gender-sensitive procedures, and timely redress to reduce underreporting and secondary victimization.

Digital literacy and cybersecurity awareness programs should be institutionalized at educational and community levels to prevent cyber offenses and empower users with knowledge of legal remedies under PECA 2016.

Public-private collaboration with financial institutions, telecom companies, and digital platforms should be strengthened to enable timely data sharing, compliance, and early detection of cyber threats.

Regular review of PECA 2016 is necessary to address emerging challenges such as artificial intelligence-based crimes, deep fakes, and cross-border cyber offenses while ensuring protection of fundamental rights.

BIBLIOGRAPHY

Internet sources

1) https://assajournal.com/index.php/36/article/view/629
2) https://jssarchives.com/index.php/Journal/article/view/260
3) https://amresearchreview.com/index.php/Journal/article/view/467
4) https://journals.centeriir.org/index.php/pjcl/article/view/102
5) https://jssarchives.com/index.php/Journal/article/view/260
6) https://amresearchreview.com/index.php/Journal/article/view/467
7) https://journals-uoli.com/index.php/SRJ/article/view/35

Books and articles

1. Cybercrime and Criminal Law in Pakistan: Societal Impact, Major Threats, and Legislative Responses
   Zahid, M., Rahman, A., and Ali, S.
2. Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan
   Khan, M. A., and Iqbal, R.
3. Digital Evidence and Procedural Fairness under the Prevention of Electronic Crimes Act 2016
   Gul, M., Ahmad, N., and Ahmad, S.
4. Unmasking Digital Deviance: Cybercrime Trends and Online Offences in Pakistan
   Suddle, M. S., Pervaiz, T., and Nawaz, H.
5. Cybercrime and Society, Yar Majid

ABBREVIATIONS

1. PECA – Prevention of Electronic Crimes Act, 2016
2. 5GW – 5th Generation warfare
3. CNSS – Committee on National Security Systems
4. PECA – Prevention of Electronic Crimes Act 2016
5. NCCS – National Center for Cyber Security
6. NCSP – National Cyber Security Policy 2021
7. ETO – Electronic Transaction Ordinance 2002
8. NR3C – National Response Center for Cybercrimes
9. ARPANET – Advanced Research Projects Agency Network

10. JANET – Joint Academic Network
11. ETO –Electronic Transactions Ordinance, 2002
12. PECO – Prevention of Electronic Crimes Ordinance, 2007
13. FATF – Financial Action Task Force