- The Electronic Transaction Ordinance 2002
- Prevention of Electronic Crime Ordinance 2008

CS204 Lesson#7_15

Lesson #7

CYBER LAWS IN PAKISTAN

- There are different laws, promulgated in Pakistan.

- These laws not only deal with crime of Internet.
- These deal with all dimensions related to computer & networks.
- Two of them are most known.
- They are: 15Aug2023
- Electronic Transaction Ordinance 2002
- Electronic / Cyber Crime Bill 2007

Electronic Transaction Ordinance 2002 15Aug2023

Overview

- The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
- Protection for Pakistani e-Commerce locally and globally.
- Protect Pakistan's critical infrastructure
- It is heavily taken from foreign law related to cyber crime.

Pre-ETO 2002 15Aug2023

- No recognition of electronic documentation
- No recognition of electronic records
- No recognition of evidential basis of documents/records
- Failure to authenticate or identify digital or electronic signatures or forms of authentication
- No online transaction system on legal basis.
- Electronic Data & Forensic Evidence not covered.
- No Rules for all of these …

Post ETO 2002

- Electronic Documentation & Records recognized
- Electronic & Digital forms of authentication & identification
- Messages through email, fax, mobile phones, Plastic Cards, Online recognized.

ETO 2002

- There are 43 sections in this ordinance
- It deals with following 8 main areas relating to e-Commerce.

1. Recognition of Electronic Documents
2. Electronic Communications
3. Web Site
4. Digital Signatures Certification Providers
5. Stamp Duty
6. Attestation, certified copies
7. Jurisdiction
8. Offences

36. Violation of Privacy Information

- Gains or attempts to gain access
- To any information system with or without any purpose
- To acquire the information unauthorized
- Imprisonment 7 years

- Fine Rs. 1 million

37. Damage to Information System

- Alter, modify, delete, remove, generate, transmit or store information
- Create hindrance in information access
- knowingly when not authorized to do so
- Imprisonment 7 years
- Fine Rs. 1 million

38. Offences to be Non-Bail able

All offences under this Ordinance shall be non-bail able, compoundable and cognizable.

39. Prosecution and trail of offences

No Court inferior to the Court of Sessions shall try any offence under this Ordinance.

Electronic/Cyber Crime Bill 2007

Overview

- "Prevention of Electronic Crimes Ordinance, 2007" is in force now

- It was promulgated by the President of Pakistan on the 31st December 2007
- The bill deals with the electronic crimes included:

1. Cyber terrorism
2. Data damage
3. Electronic fraud
4. Electronic forgery
5. Unauthorized access to code
6. Cyber stalking
7. Cyber Spamming/spoofing

- It will apply to every person who commits an offence, irrespective of his nationality or citizenship.
- It gives exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes.

Punishments

Every respective offence under this law has its distinctive punishment which can be imprisonment or/and fine.

Sections

Damage:

Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.

Punishment:

- 3 years

- 3 Lac

Electronic fraud:

People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm.

Punishment:

- 7 years
- 7 Lac

Electronic Forgery:

Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic.

Punishment:

- 7years
- 7 Lac

Malicious code:

Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or device, with intent to cause harm to any electronic system or resulting in the theft or loss of data commits the offence of malicious code.

Punishment:

- 5 years
- 5 Lac

Cyber stalking:

- Whoever with intent to harass any person uses computer, computer network, internet, or any other similar means of communication to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image.
- Threaten any illegal or immoral act
- Take or distribute pictures or photographs of any person without his knowledge
- Commits the offence of cyber stalking.

Punishment:

- 3 Years
- 3 Lac

Spamming:

- Illegal electronic messages to any person without the permission of the recipient.

Punishment:

- 6 month
- 50,000

Spoofing:

Whoever establishes a website, or sends an electronic message with a fake source intended to be believed by the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information

Punishment:

- 3 Years
- 3 Lac

Offence	Imprisonment (years)	Fine
Criminal Access	3	3 Lac
Criminal Data Access	3	3 Lac
Data Damage	3	3 Lac
System Damage	3	3 Lac

Electronic Fraud	7	7 Lac
Electronic Forgery	7	7 Lac
Misuse of Device	3	3 Lac
Unauthorized access to code	3	3 Lac
Malicious Code	5	5 Lac
Defamation	5	5 Lac
Cyber stalking	3	3 Lac
Cyber Spamming	6 months	50000
Spoofing	3	3 Lac
Pornography	10	-------
Cyber terrorism	Life	10 Million

Criticism

- There are seemingly 21 ‘cyber’ issues covered in this Bill.
- It may seem to cover all aspects of the new digital era.
- But detailed look shows quite the contrary.
- Practically in all issues the government has gone the extra mile to reinvent a new definition, significantly deviating from the internationally accepted norms.
- There seems to be an elaborate play of words within the document
- allow room for the regulating body (FIA) to confuse and entrap the innocent people
- The FIA, has been given complete and unrestricted control to arrest and confiscate material as they feel necessary
- A very dangerous supposition
- Safeguards and Protection

One example of the hideous nature of the bill:

- The Government has literally attempted to insert a new word in the English language.
- The word TERRORISTIC is without doubt a figment of their imagination vocabulary
- Hence they attempt to define the word, quite literally compounding the problem at hand
- They have actually defined what real-life terrorism might be
- But fail to explain what they mean by the word Cyber in cyber terrorism.
- The concern is that there happens to be no clear-cut explanation on how a Cyber Terrorism crime is committed.

Why we must know Cyber Laws?

- Which specific laws apply to Organization.
- By law, which information assets need to be protected?
- Organizational Policies and Rules.

Lesson #8

CONCEPT OF CYBER SPACE JURISDICTION AND OTHER PRINCIPAL OF JURISDICTION

Jurisdiction

The right, power, or authority to administer justice by hearing and determining controversies.

- Territorial Jurisdiction
- Extra Territorial Jurisdiction
- Cyber Jurisdiction

Territorial Jurisdiction

It refers to jurisdiction over cases arising in or involving persons residing within a defined territory.

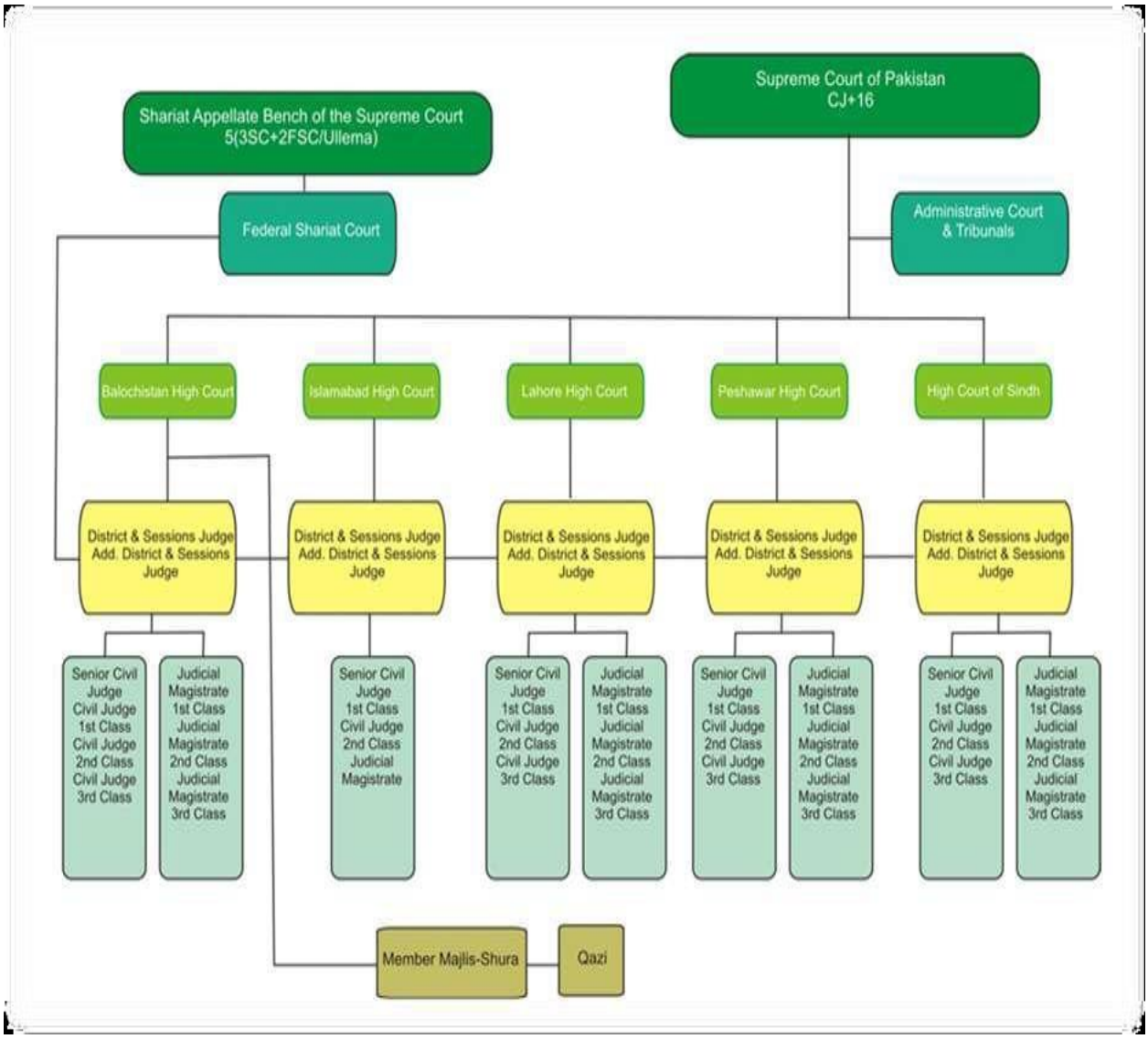
Extra Territorial Jurisdiction

15Aug2023

Extra territorial Jurisdiction refers to a court's ability to exercise power beyond its territorial limits.

Cyber Jurisdiction

A virtual approach, defining the cyber world beyond the boundaries of nation states enforcement of cyber laws uniformly accepted.



Cyber Dispute/Conflict

A tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks may result in retaliation.

Lesson #9

INTELLECTUAL PROPERTY RIGHTS, PRIVACY AND FREEDOM OF SPEECH

Concept of Virtual Property

- An emerging property form – virtual property – that is not intellectual property, but that more efficiently governs rivalrous, persistent, and interconnected online resources.
- Examples include URL; email address, IP address etc.
- Virtual property is govern through the law of intellectual property

Rivalrousness, in the physical world, lets the owner exclude other people from using owned objects we often desire the power to exclude in cyberspace too, and so we design that power into code. By design, we make code that can only be possessed by one person. Thus, rivalrousness exists also in code. If one person controls rivalrous code, nobody else does. For example, no one but the owner of an internet address (or those the owner permits) can post content to that address. If person A owns a given internet address, person B cannot put her website up at that address. If one person has a given email address, nobody else can receive mail at that same address.

Persistent: For example, an email account can be accessed from a laptop, a desktop, or the local library. When an email account

owner turns her laptop off, the information in that account does not cease to exist. It persists on the server of her Internet Service Provider.

- Objects in the real world are also naturally interconnected. Two people in the same room experience exactly the same objects. Objects in the real world can affect each other, by the laws of physics. Similarly, code can be made interconnected, so that although one person may control it, others may experience it. The value of a URL or an email address is not solely that the owner can control it; the value is that other people can connect to it, and can experience it. They may not be able to control it without the owner's permission, but – as with real estate in the real world – with the owner's invitation they may interact with it.
- Amazon as virtual property.

Trademarks

- A symbol, word, or words legally registered or established by use as representing a company or product.
- In cyber world URL's are more like trademarks
- Provides the rights of the owner of a name, symbol, and mark for protection to avoid consumer confusion. This applies specifically in the acquisition of domain names that are appropriate for a business' trademark. Trademark protection has typically resided at the nation state level, and the global nature of the internet has caused problems with

the use of certain domain names. A secondary issue is the difference in countries with respect to "first to use" versus "first to file".

- Consumer Protection Act, 15 U.S.C. § 1114, 1125(a) (2000)
- **Cyber squatting**: is the behavior of acquiring a domain name with the intention of reselling to a third party which has a higher perceived value for that name, or to exploit 'traffic' that domain name generates based on consumers' presumption of the purpose of the domain name.

Copyrights 15Aug2023

- Provision to own over a specific period of time
- Examples are books, music, research journals, website etc.
- License is description given by the owner on how to use the property
- Copy right protection
- Fair use Clause
- Expansion of Top Level Domains (TLD's).

Patents 15Aug2023

- A patent is a government authority or license conferring a right or title for a set period, especially the sole right to exclude others from making, using, or selling an invention
- Patent Right
- Patent Ordinance
- Patent Rules

- Patents Granted by IPO (Intellectual Property Organization of Pakistan)
- Patents Expired

Data Protection Laws

- Data protection laws are to provide protection to electronic data with regard to the processing of electronic data
- Pakistan Data Protection Act 2005
- Advantages of Data Protection Act
- Disadvantages of Data Protection Act

Lesson #10

ESTABLISMENT OF INVESTIGATION AND PROSECUTION AGNECIES

Cyber Crime

One of the largest computer security companies, Symantec Corporation, defines cybercrime as "Any crime that is committed using a computer or network, or hardware device".

Existing Strategies and Cybercrime in US 15Aug2023

- Department of Defense Strategy for Operating in Cyberspace
- Strategy to Combat Transnational Organized Crime
- International Strategy for Cyberspace
- National Strategy for Trusted Identities in Cyberspace
- Council of Europe Convention on Cybercrime
- National Strategy to Secure Cyberspace

National Response Centre for Cyber Crimes (NR3C)

Responsibilities: 15aUG2023

Some of the responsibilities are listed below

- Enhance the capability of Government of Pakistan and Federal Investigation Agency to effectively prevent growing cyber crimes.
- Reporting & Investigation Centre for all types of Cyber Crimes in the country.

- Liaison with all relevant national and international organizations to handle cases against the Cyber Criminals.
- Provide necessary technical support to all sensitive government organizations to make their critical information resources secure.
- Carry out regular R & D activities to make the Response Centre as a centre of technical excellence.
- Provide timely information to critical infrastructure owners and government departments about threats, actual attacks and recovery techniques. A role of Computer Emergency Response Team (CERT).
- To provide on demand state-of-the-art electronic forensic services and cyber investigative to support local police.

Power of Officers

Subject to provisions of Cybercrime Bill 2015 Act, an investigating officer shall have the powers to :

- Have access to and inspect the operation of any specified information system.
- Use or cause to be used any specified information system to search any specified data contained in or available to such information system.
- Obtain and copy any data, use equipment to make copies and obtain an intelligible output from an information system.
- Have access to or demand any information, code or technology which has the capability of retransforming or

unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version.

- Require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any information system has been used to grant access to any data within any information system within the control of such person.

- Require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the investigating officer may require for investigation of an offence under this Act; and

- Require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

Real Time Collection of Traffic Data

Many organizations and defense industry base, have discovered that while traditional security monitoring systems can help information assurance efforts, they are rarely enough to react to today's external, targeted, persistent, zero-day attacks. As a result, leading agencies and some private sector organizations are beginning to replace point-in-time audits and compliance checks with a continuous monitoring program to help them prioritize controls and provide visibility into current threats.

Retention of Traffic Data 15aug2023

The policy for retention of Traffic data Under Pakistan Electronic Crime act 2015 is as follows

- A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of ninety days or such period as the Authority may notify from time to time and provide that data to the special investigating agency or the investigating officer whenever so required.
- The service providers shall retain the traffic data under sub section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).
- Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to or with both.

Warrant for Disclosure of Data

The policy for warrant for disclosure of data Under Pakistan Electronic Crime act 2015 is as follows

- Upon an application by an investigating officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that specified data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data to provide such data or access to such data to the investigating officer.

- The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes an extension for a further period of time as may be specified by the Court.

Lesson #10

PROSECUTION AND TRAIL OF OFFENCES

Offence to be Compoundable and Non-Cognizable

CYBER OFFENCES 15Aug2023

There are about 19 cyber offences defined in Pakistan Ordinance No. LXXII or 2007 to make provision for prevention of the electronic / cyber crimes.

OFFENCES

- Criminal Access
- Cyber Stalking
- Spamming
- Spoofing
- Unauthorized Interception
- Cyber Terrorism
- Criminal Data Access
- Unauthorized Access to Code
- Misuse of Encryption
- Malicious Code
- Enhanced Punishment For Offences Involving Sensitive
- Data Damage
- System Damage
- Electronic Fraud
- Electronic Forgery
- Misuse of Electronic System or Electronic Device
- Offences By Corporate Body

Prosecution and Trail of Offenses

15Aug2023

It is critically important to explore factors delaying investigation and prosecution of cyber crime offending to raise awareness and expose these barriers to justice.

- Criminal Activities Perpetrated Electronically
- Law Enforcement and Policing
- Investigating Cyber Crime
- Impediments to Evidence Discovery and Analysis

Order for Payment of Compensation

15Aug2023

- Punishment of Imprisonment
- Fine
- Compensation To Victim

Lesson #12

PREVENTION MEASURES FOR CYBER CRIMES

Cyber Crime Cases

15Aug2023

- Thursday, 13-Sept-2012
  2 Cyber Criminals arrested in Bahawalpur

- Cyber Crimes against Pakistani women

- January 02, 2016
  FIA cyber crime lodges first case of 2016

Protection of Credit Cards and Bank Accounts

- Credit Card Safety First
- Keep Your Account Number Private
- Be Careful with Your Receipts
- Be Sure Your Device and Networks Are Secure
- Think Credit Card Protection When Shop Online
- Keep Your Password Secret
- Check Your Account Often
- Report Loss Card and Suspected Fraud Right Away

Secure IT Infrastructure 15Aug2023

Logical Network Security Segmentation

- Network Security Zones
- Restricted Zone
- Management Zone

Security Event Logging

Network Intrusion Detection and Prevention Systems

Packet Capture

Password Policy

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

- Password Protection
- Password Requirements
- Choosing Passwords

Awareness for Staff and Organization 15Aug2023

Awareness learning needs to enter the 21st Century

-
- 45% unintentional Error by Employees or Contractors.
- 40% Intentional Attacks by Employees or Contractors.
- 17% Third party suppliers or joint venture partners as a route exploited by cyber criminals.

Lesson #13

CYBER SECURITY STRATERGIC PLANNING FOR PAKISTAN

Challenges

- CYBER AWARENESS
- LACK OF CYBER AWARENESS
- NATIONAL CYBER SECURITY FORUM
- ABSENCE OF REGIONAL COOPERATION
- DIGITAL RIGHTS AND OBLIGATION
- CYBER CENSORSHIP
- UNCHECKED HACKTIVISM

Cyber Awareness

- Cyber security has yet to blip on the national radar.
- No political party has included it on its manifesto.
- No legislation on cyber issues in the parliament.
15Aug20223
- Police department, judiciary & lawyers have little/no knowledge and experience in investigating & prosecuting digital crimes.
- No chamber of commerce runs any cyber security course or gives advice to businesses to secure their digital enterprises.
- No policy in preventing import of hardware with embedded technologies.
- None of the government agency, electronic media, higher education institute has a cyber security policy.
- Digitally advanced countries organize cyber awareness days/weeks.

Lack of Natural Cyber Policy

- National cyber mandate & division of turf among multiple stakeholders i.e. It ministry, moi, most, mod, js hq, int agencies.
- National cyber strategy – issues such as protection of critical infrastructure & response to computer emergencies.
- Cyber terrorism.
- Cyber criminal code.
- Laws to regulate online businesses.
- Cyber censorship – rules & policies.
- Foreign policy

– How to respond diplomatically to cyber incidences.

– Policy for delegates attending the GGE conferences at the UN, internet governance conferences & international seminars.

– Policy guidelines for engagement with ITU.

Defense policy

– how to react to various kinds of attacks.

Natural Cyber Security Forum

15Aug2023

Government to create a national cyber security forum and designate lead ministry /Agency.

- Lead ministry to publish a national calendar for holding cyber security seminars.
- Lead ministry to organize national cyber security drills more than once annually.
- Lead ministry to run courses for parents to digitally monitor their children.
- Universities to group together to promote cyber security education under the umbrella of the HEC.

Absence of Regional Co-Operation

- Countries are cooperating jointly and en bloc in cyber security issues i.e. Asian is very active in this regard.
- There is no bilateral or regional cooperation in South Asia. SAARC can provide an important forum for cyber security.

Digital Rights and Obligations

Is our Government aware of its national digital obligations?

- In matters like enforcing unconventional on right of children (UNRC) preventing children pornography through digital means.

What are a citizen's digital rights?

- To access all kinds of websites.

What are the citizen's obligations?

- To prevent cyber bullying/sexual harassment & reporting illegal activity in cyber space.

Cyber Censorship 15Aug2023

Cyber censorship is of what can be accessed, published, or viewed on the Internet. Cyber censorship can be implemented by:

- National policy for handling digital incidents e.g. The YouTube incident.
- Stronger filters for pornographic sites.
- Efficient mechanisms to control preventing spread of hate literature & operations of prohibited organizations.

Unchecked Hacktivism

- Uncontrolled hacktivism now forms part of the India Pakistan rivalry.
- Independent group of hackers with colorful names like Pakistan cyber army, Indian cyber army, Pakistan hackers club, Pakhaxors, predators PK, Hindustan hacker's organization defaces an Indian or Pakistani website.
- Mostly the homepage is littered with poorly- worded patriotic statements and taunts that often provoke the other nation's hacking groups to retaliate.
- The homepage is defaced and replaced with juvenile comments. Often, these hackers block visitors' access to important information. Such acts, of course, lead to more cyber defacements, with the most "coveted" targets being government websites. A cyber-attack is usually triggered by some act of violence or aggression from the rival country. Within a span of hours, these groups of hackers locate a

high-value website that doesn’t have adequate cyber security in place, and gains root access to the web server by hacking into it.

Reference

KTH-SEECS Applied Information Security (AIS) Lab

Lesson #14

CYBER CRIME AND LAW: INTERNATIONAL PROSPECTIVE

What is a gTLD? 15Aug2023

15Aug2023

- A gTLD is a generic top level domain. It is the top-level domain of an Internet address, for example: .com, .NET and .org.
- In addition, seven new gTLDs were also selected by ICANN (the Internet Corporation for Assigned Names and Numbers) on November 16, 2000.

15Aug2023

These are:

- .aero (for the entire aviation community)
- .biz (for business purposes)
- .coop (for cooperatives)
- .info (unrestricted)
- .museum(for museums)
- .name (for personal names)
- .pro (for professionals).

What is a ccTLD?

- A ccTLD is a country code top-level domain, for example: .mx for Mexico.

- These ccTLDs are administered independently by nationally designated registration authorities.
- There are currently 252 ccTLDs reflected in the database of the Internet Assigned Numbers Authority (IANA).
- WIPO, which has a ccTLD Program, has launched a database portal, facilitating online searches for information related to country code top level domains.

International Cyber Crime

- There is no commonly agreed single definition of “cyber crime”.
- It refers to illegal internet-mediated activities that often take place in global electronic networks.
- Cyber crime is "international" or "transnational" – there are ‘no cyber-borders between countries'.
- International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement.

International Jurisdiction

- International jurisdiction refers to the fact that the courts of a given country will be the most appropriate to hear and determine a case that has an international dimension.
- A dispute has an international dimension where, for example, the parties have different nationalities or are not resident in the same country.

- In such a situation the courts of several countries might have jurisdiction in the case, and we have what is known as a conflict of jurisdiction.
- The rules of international jurisdiction lay down criteria for determining the country whose courts will have jurisdiction in the case.

Convention on Cyber Crime

- The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention.
- It is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.
- It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, South Africa and the United States.

Role of ICANN in Internet Regulation

- To reach another person on the Internet you have to type an address into your computer -- a name or a number. That

address must be unique so computers know where to find each other.

- ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet.
- In more technical terms, the Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS).

The IANA functions include:

- The coordination of the assignment of technical protocol parameters including the management of the address and routing parameter area (ARPA) top-level domain
- The administration of certain responsibilities associated with Internet DNS root zone management such as generic (gTLD) and country code (ccTLD) Top-Level Domains.
- The allocation of Internet numbering resources; and other services. ICANN performs the IANA functions under a U.S. Government contract.

Lesson# 15

CYBER LAW COMPLIANCE

Challenges

- Need of Cyber Law
- Laws of Electronic Transactions
- Electronic Transactions Ordinance 2002
- International Consensus Principles
- Cyber Laws Situation in Pakistan

Need For Cyber Law

- Trade and business communications through electronic means give rise to a number of legal issues.
- For instance if a service were sold over the Internet across countries, in which geographical location can the transaction be deemed to have occurred? This question may be important from the point of view of consumer protection and establishing jurisdiction.
- Furthermore electronic transactions require electronic contracts and electronic signatures which have not been provided for in the contract laws of many countries. Most countries that wished to participate in electronic commerce needed to undertake major legislative reforms in this regard.

Law for Electronic Transaction

- United Nations Commission on International Trade Law (UNCITRAL) is a core legal body of United Nations with universal membership, specializing in commercial law reform.
- In order to increase trade worldwide, UNCITRAL is formulating modern, fair, harmonized rules on commercial transactions, including;
- Conventions, model laws and rules that are acceptable worldwide.
- Legal and legislative guides and recommendations of great practical value.
- Technical assistance in law reform projects.

A report was prepared by the UNCITRAL experts on "Legal value of computer records" and based on that report the Commission adopted the following recommendations to states to review legal requirements:

- Affecting the use of computer records as evidence in litigation.
- That certain trade transactions or trade related documents be in writing.
- Necessitate handwritten signature or other paper-based method of authentication on trade related documents; and
- Those documents for submission to governments are in writing and manually signed.

Electronic Transaction Ordinance 2002

Government of Pakistan adopted its IT Policy in the year 2000 and after studying UNCITRAL model laws, looking at various legislations of both Civil and Common law countries, reviewing different implementation schemes of electronic authentication, regulatory models and best practice guidelines and appreciating the above-mentioned three approaches being followed all over the world, has followed the "International Consensus Principals on Electronic Authentication" designed by Internet Law and Policy Forum and "two-tier" approach.

Two Tier Approach

- Some jurisdictions have begun to realize that first two approaches are not necessarily mutually exclusive, and so have adopted "two tier" approach representing convergence and synthesis of the first two approaches.
- This consolidated approach generally takes the form of enacting laws that prescribe standards for operation of PKIs, and concurrently take a broad view of what constitutes a valid electronic signature for legal purposes.
- This "two-tier" approach has found increasing support, most notably in the European Union and Singapore.

International Consensus Principles

International Consensus Principles prepared by Internet law and Policy Forum (ILPF) in Sept' 2000 to create a predictable legal environment are as below:

- Remove legal barriers to electronic authentication.
- Respect freedom of contract and parties' ability to set provisions by agreement.
- Harmonization: make laws governing electronic authentication consistent across jurisdictions.
- Avoid discrimination and erection of non-tariff barriers.
- Allow use of current or future means of electronic authentication.

Cyber Law Situation in Pakistan

15Aug2023

Overall the situation of cyber laws is very encouraging in Pakistan and we are ahead of many developing countries in this respect.

The Analysis of the above laws shows that:

- There should be some well-coordinated effort to critically review drafts already prepared.
- Prepare drafts of remaining required laws with single focal point in the Federal Government to avoid conflicts, overlapping and gaps.