# Cs204 Grand Quiz Fall 2020

1. When a customer of a website are unable to access it due to bombardment of fake traffic, it is known as
   - Denial of Service Attack
2. Security Procedure can
   - Reduce but not eliminate risks
3. How Many Issues are covered In Electronic Crime Bill 2007 ?
   - 21
4. A tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks may result in retaliation termed as
   - Cyber Dispute
5. The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation that consisted of sections.
   - 43
6. The 1st Law related to cyber issues 1st introduced in ----------
   - 2002
7. When Plain text is converted to unreadable format, it is termed as -----.
   - Cipher Text
8. Which of the following is an example of a cyber crime?
   - Spam Emails
9. What Floods a website with so many request for service that it slows down or crashes ?
   - Denial-of Service attack
10. Malicious software is known as
    - Malware
11. A cyber attach in which a minor fraction of priced is added and taken to some other account is called..
    - Forgery
12. The First Cyber regulation was evolved in the year ----------
    - 1966
13. Jurisdiction over cases arising in or involving persons residing within a defined territory refers to ---------
    - Territorial Jurisdiction
14. All of these are suggestion for safe computing EXCEPT
    - Open all e-mail messages but open slowly
15. What is the fine of the “Cyber Spamming” Offense according to Electronic Crime Bill 2007?
    - 50,000
16. Which of the following is a goal that courts try to achieve?
    - All of the Given Options
17. -------is defined as any crime completed through the use of computer technology
    - Computer Crime
18. Cyber Culture Language is -----
    - No specific Language
19. According to Electronic Crime Bill 2007 what is the imprisonment of “Unauthorized access to code” Offense ?
    - 3 Years
20. -------- are the building blocks of the website.
    - Web pages

21. In ---------- the dimensions are physical in nature and all transactions are Performed off-line?
    - Traditional Commerce
22. According to Electronic Crime Bill 2007 what is the imprisonment of “Criminal Access” Offense?
    - 3 Years
23. How many sections are included in Electronic Transactions Ordinance 2002?
    - 43
24. What is the most common tool used to restrict access to a computer system?
    - Passwords
25. Virus can reach to your computer in which way?
    - All of the above
26. What is the fine of “Defamation” Offence According to Electronic Crime Bill 2007?
    - 5 Lac

27 --------is the process or mechanism used for converting ordinary plain text into garbled non-
human readable text & vice versa.

- Cryptography

28. Members of Majlis-e-Shura in Shariah Appellate bench of supreme court of Pakistan works under ?
    - Supreme Court
29. In ---------- the dimensions are digital in nature and all transactions are performed on-
line
    - Pure E-commerce
30. Internet is Owned by
    - No Body owns internet
31. The term “Cyber Law” Refers to all the legal and regulatory aspects of ----the and its ----
    - Internet , users
32. Who breaks into other people’s computer systems and steals and destroy information?
    - Hackers
33. Public key cryptography is also known as-------Cryptography?
    - Asymmetric
34. What is “I” stands in CIA triad?
    - Integrity
35. What is short for malicious software ( is a software designed to disrupt computer operations, gather sensitive information ,or gain unauthorized access to computer systems)?
    - Malware
36. The 1st l law related to digital transaction in Pakistan was introduced in --.
    - 2002
37. Firewalls are used to protect against ---- --.
    - Unauthorized Access
38. Model Law on E-Commerce and E-Signatures were evolved in -----.
    - 1996
39. The network formed by the co-operative interconnection of a large number of computers networksis called --.
    - Internet

40. Amazon.com comes under the following model?
    - B2C
41. The imprisonment under section for violation of privacy information is ---- with fine of ----
    - 7 years. 1 million
42. Each electronic document on the web is called a ----------
    - Web Page
43. What is hardware and/or software that protects computers from intruders?
    - Firewall
44 -------- is a discussion or informational site published on the World Wide Web consisting of
    discrete entries typically, runs by an individual or a small group
    - Blog
45. What is the process of making a copy of the information stored on a computer?
    - Backup
46. In a hybrid approach ----- key is used to decrypt session key and key to decrypt ciphertext
    - Private, Session
47. There are----- types of Jurisdiction
    - 3
48. Gains or attempts to gain access to any information system with or without any purpose comes under ----------
    - Violation of Privacy information
49. Which type of e-commerce focusses on consumers dealing with each other?
    - C2C
50. What is the fine of “Cyber Terrorism” Offense According to Electronic Crime Bill 2007 ?
    - 10 Million
51. Process of buying, selling or exchanging products, services and information through computer networks is called
    - E-commerce
52. E-commerce is not suitable for
    - Online Job Searching
53. An e-business that allows consumers to name their own price for product and service is following which e-commerce model
    - C2B
54. Most individuals are familiar with which form of e-commerce ?
    - B2C
55. Which Process can Prevent data from lose due to computer problems or human errors?
    - Backup
56. The ability of a court to exercise power beyond its territorial limits refers to ---------- Jurisdiction.
    - Extra Territorial Jurisdiction
57. The practice of forging a return address on an e-mail, so that the recipient is fooled into revealing private information is termed as?
    - Spoofing
58. What software detects and removes computer viruses
    - Antivirus
59. In internet terminology IP means
    - Internet Protocol

60. The right, power, or authority to administer justice by hearing and determining controversies is referred to as?
    - Jurisdiction
61. What scrambles the contents of a file so you can't read it without having the right decryption key?
    - Encryption
62. collecting personal information and effectively posing as another individual is known as
    - Identity Theft
63. The method of hiding ----in such a way as to hide its substance is called encryption
    - Palin-text
64. Territorial Jurisdiction Refers to Jurisdiction over cases arising in or involving persons residing within a--------.
    - defined territory
65. in--- both ends must agree upon a single shared key for encryption and decryption of messages and keep the key secret between them
    - Symmetric Encryption
66. The first Cyber regulation in Pakistan was------ --.
    - Electronic Transaction Ordinance
67. What is "A" Stands for in CIA triad?
    - Availability
68. What is "C" Stands for in CIA triad?
    - Confidentiality
69. Who Protects system from external threats?
    - Firewall
70. All the legal and regulatory aspects of the Internet and its user are defined in the term
    - Cyber Law
71. A website is being accessed by referencing a that identifies the site
    - Uniform resource locator (URL)
72----------Cipher technique uses "shift by 3 "rule in encrypting the plain text.
    - Caesar Cipher

## Cs-204

## Mcq's

**1)** World Wide web is the collection of **electronic documents.**

**2)** Each electronic document on the web is called a **web page** that can contain text, graphics, audio and video**.**

3) **Cyber Culture** converts the human written language or symbols to machine language and reconverts to human understandable language so the people on the destination can understand.

4) Now a day's especially in online chatting cyber language is created of

new

codes which affect our daily **spoken language**.

5) There are **Seven** components of cyber culture.

6) Internet, email, blog, chat, e-commerce, social networks and website are

components of **cyber culture.**

7) **Internet** is The network formed by the co-operative

interconnection of a large number of computer networks.

8) **Main goal** of the internet is to connect several computers together

for the exchange of messages and share the information etc.

9) **Website** is a location connected to the Internet that maintains one

or more web pages.

10) Web pages are the **building** blocks of the website

11) Web sites may be accessible through a **public Internet Protocol (IP)** network, such as the Internet, or a private local area network (LAN), by referencing a uniform resource locator (URL) that identifies the site.

**12)** Email stands for **Electronic mail.**

13) There is no central **administration** and owner to the internet.

14) Messages that are sent electronically from one computer to another is an e-mail **message.**

15) A **blog** is a discussion or informational site.

**16)** Blog is published on the World Wide Web and consists of **discrete entries** ("posts").

**17)** A regularly updated website or web page is run by an **individual or group of individuals.**

18) Any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver is called **online chat**

19) Online chat may address **point-to-point communications** as well as **multicast communications.**

20) Chat can be from one sender to many receivers and video chat, or may be a **feature** of a web conferencing service.

21) A chat may **be direct text-based or video-based (webcams**)

**22)** E- commerce stands for **Electronic Commerce.**

23) **E-commerce** is the trading or facilitation of trading in products or services using computer networks, such as the Internet.

24) Online shopping, online market places, Business to business buying &

selling, online newsletter for marketing prospective are **Commercial transactions** on internet**.**

25) A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages,

images , videos are referred to as **social networks.**

**26)** Facebook, Linkedin, Twitter are examples of **Social network.**

27) The **cyberspace** is a term used to describe the space created through the union of electronic communications networks such as the internet, which enables computer facilitated communication between any numbers of people who may geographically dispersed around the globe.

28) Cyberspace is a **public space** where individuals can meet, exchange ideas, share information, provide social support and conduct business.

29) “The human interaction does not require physical connection to communicate, but is rather characterized by the interconnection of millions of people throughout the world through chat room, email,

Facebook” is the

concept of **Cyber space**.

30) Due to **worldwide** use of computer network, people are now able to

get together and form **cyber communities** that can exchange messages easily through cyber space.

**31)** Physically meeting has been reduced due to introduction of **cyber culture**.

32) **Culture** is an **important** process in computer related contexts. The processes that create meaning in actions.

33) Cyber culture is indicated to break down borders and barriers, not

only between nations but also between groups and individuals **separated**

from each other due to some reasons.

34) If cyber culture grows then those who are cut off from cyber culture

will feel more **isolated** from society and will not be properly updates about latest development and fast change.

35) The **cyber culture** has brought great impact on human individual'slife.

36) ducation the style of teaching learning has changed. The student teacher **interactivity** can be formed **online**.

37) The cyber culture has great influence in the **business world**.

38) The use of internet for emails and other social networks is our **participation in the cyber culture.**

39) Cyber culture **reduced** the gap between groups and individuals separated from each other due to some reasons.

40) Now days there are many social networking sites like Face book, MySpace and Twitter, which all serve to provide **links** to many friends to **maintain** their relationship.

**41)** Face to face communication is becoming weak due to **emerging of social networks.**

42) The People who **don't have the ability to communicate face to face** they can exchange their views, through these social network.

43) The cyber culture is **developing** and we **need** to know the values and believes of this culture.

**44)** Cyber culture has great influence on human culture and in way **new uniform global culture is developing.**

45) In traditional E-commerce all the dimensions are **physical** in nature.

46) In Pure E- commerce all the dimensions are **digital** in nature.

47) **Hacking** in simple terms means illegal access into a computer system without the permission of the computer owner/user.

48) Damaging or destroying data rather than stealing or misusing them is called **cyber vandalism**.

49) A **Virus** is a “program” that is loaded onto your computer without your knowledge and runs against your wishes.

50) **Trojan horses** are email viruses that can duplicate themselves, steal information, or harm the computer system.

51) The method of hiding plaintext in such a way as to hide its substance is called **encryption**.

52) The term **“Cyber Law”** Refers to all the legal and regulatory aspects of the Internet and its users.

53) The 1st rule of management is **delegation**.

54) The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by **national lawmakers**.

55) 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.

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

57) Awareness learning needs to enter the **21st** Century.

58) A **gTLD** is a generic top level domain.

59) A **ccTLD** is a country code top-level domain, for example:

.mx for Mexico.

60) There are currently **252** ccTLDs reflected in the database

of the Internet Assigned Numbers Authority (IANA).

61) **B2B** Model describes commerce transactions between businesses,

such as between a manufacturer and a wholesaler, or **between a wholesaler**

**and a retailer**.

62) The **B2C** model involves transactions between business organizations

and **consumers**.

**63)** A **C2B** model, is a type of commerce where a consumer or **end user**

provides a product or service to an organization.

64) Computer may be used as a **weapon** for crime or as a target.

65) **Cyber security** refers to the technologies and processes

designed to protect computers, networks and data from

unauthorized access and attacks delivered through the Internet by

cyber criminals.

66) Security deal with **three** primary issues, called the **CIA** triad.

67) **Malware** is any software that infects and damages a computer

system without the owner's knowledge or permission.

68) **Trojan horses** are email viruses that can **duplicate**

themselves, steal information, or harm the computer system.

69) The method of hiding plaintext in such a way as to hide its substance

is called **encryption**.

**70)** **Encrypting** plaintext results in unreadable gibberish **called cipher**

**text.**

71) The term **Cyber Law** Refers to all the legal and regulatory

aspects of the Internet and its users.

**72)** There are **43** sections in the ordinance **ETO 2002**. It deals with the **8**

main areas relating to e-Commerce.

73) Illegal electronic messages to any person without the permission of

the recipient is called, **Spamming**

74) A tense situation between and/or among nation-states and/or

organized groups where unwelcome cyber attacks may result in

retaliation

is, **Cyber dispute / conflict**

75) A virtual approach, defining the cyber world beyond the boundaries of

nation states enforcement of cyber laws uniformly accepted, **Cyber**

**Jurisdiction**

76) There are_____domains of E-commerce.

- **2**
- **3**

- **4**

- **5**

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

78) How many sections are included in Electronic Transaction Ordinance 2002?

- **43**
- 10
- 53
- 23

79) Public key encryption uses multiple keys. One key is used to encrypt data, while another is used to decrypt data. The key used to encrypt data is called the___key, while the key used to decrypt data is called the

___key.

- Encryption, decryption
- Private, public
- Encryption, public
- **Public, private**

80) What is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient?

- Encryption

- **Public key encryption**
- Intrusion-detection software
- Security-auditing software

81) The term Cyber Law is refer to as the legal and regulatory aspects of the_____and its____.

- Users, Internet
- **Internet, Users**
- Digital data, Generators
- Internet Service Provider, User

82) According to Electronic Crime Bill 2007 what is the imprisonment of “Unauthorized access to code” Offense?

- 6 Years
- **3 Years**
- 3 Months
- None of the above

83) According to Electronic Crime Bill 2007 what is the imprisonment of “Electronic Fraud” Offense?

- 1 Year
- 10 Months
- **7 Years**

- 7 Months

84) What scrambles the contents of a file so you can't read it without having the right decryption key?

- **Encryption**
- Intrusion-detection software
- Security-auditing software
- All of the above

85) What is the Fine of "Cyber Terrorism" Offense according to Electronic Crime Bill 2007?

- 1 Million
- **10 Million**
- 10 Thousand
- None of the above

86) What is the fine of "Defamation" Offense according to Electronic Crime Bill 2007?

- 5000
- 50,000
- **5 Lac**
- 7 Lac

87) What is the Fine of “Cyber Spamming” Offense according to Electronic Crime Bill 2007?

- **50,000**
- 35,000
- 5 Lac
- None of the above

88) Cyber security refers to the **technologies** and **processes** designed to protect computers, networks and data from unauthorized access and attacks delivered through the Internet by cyber criminals.

89) We can Use our computers to **attack** other computers on the internet.

90) **Security measures** provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the **dynamic** threats posed by cyber thieves and cyber terrorists.

91) **Trojan horses** are such programs which are used as the **back doors**.

92) Security suites, such as **Avast Internet Security**, will prevent you from downloading Trojan Horses.

93) **Password attacks** are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

94) **Cyber security** is necessary since it helps in **securing data** from threats such as data theft or misuse, also safeguards your system from **viruses.**

95) **Security measures** provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the **dynamic threats** posed by cyber thieves and cyber terrorists.

96) Your **home computer** is the popular **target** for intruders.

97) **Hackers** attack where they see **weakness**.

98) A system that hasn't been **updated** recently has flaws in it that can be taken advantage of by **hackers**.

99) The word "**malware**" comes from the term "**Malicious software**."

100) Main goal of the **internet** is to connect **several computers** together for the **exchange** of messages and share the information etc.

.....

1. **Positive Online Environment of Internet users and a healthy cyber culture for the Internet community**
2. A **recognition** of the power of the Internet to benefit oneself and the community at large.
3. To **reflect** on how to become a responsible user of social networking sites and a commitment towards building a healthy cyber culture
4. Focuses on the construction, maintenance and facilitation of community in **electronic** networks and computer mediated communication.
5. **World Wide Web** is the collection of electronic documents.
6. **Each electronic document on the web is called a web page.**
7. Web page can contain **text, graphics, audio and video**.
8. **The use of World Wide Web by a people or a group of people for the exchange of social expectations, custom, history and language iscalled cyber culture.**
9. Like every culture has its own **language**,
10. the cyber culture is not the **exception** to this rule.
11. It converts the human written language or symbols to **machine language** and reconverts to human understandable language so the people on the destination can understand.
12. Now a day's specially in online chatting the cyber language is creates of new **a code which affects** our daily spoken language.

13. The network formed by the co-operative **interconnection** of a large number of computer networks.
    No one **owns the Internet**.
    There is **no central administration** to the internet.
14. Main goal of the internet is to **connect several computers together** for the exchange of messages and share the information etc.

Community of people.
Collection of
resources.

15. A location connected to the **Internet** that maintains one or more web pages.

16. Web pages are the **building blocks** of the website.

**17.** Web pages includes documents like **texts and multimedia contents**

**18. A web sites may be accessible through a public Internet Protocol (IP) network, such as the Internet, or a private local area network (LAN), by referencing a uniform resource locator (URL) that identifies the**
site.

**19. Electronic mail**, most commonly called **email.**

**20. E-mail is the Most widely used application on the internet.**

**21. Messages that are sent electronically from one computer to another is an e-mail message**

22. A **blog** is a discussion or informational site published on the World Wide Web consisting of discrete entries ("posts").

**23.** A regularly updated website or web page, typically , runs by **an individual or a small group**

**24. Any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver is called online chat.**

**25.** Online chat may address **point-to-point** communications as well as multicast communications from one sender to many receivers and video chat, or
may be a feature of a web conferencing service.

**26.** Any **direct text-based or video-based** (webcams), one-on-one chat or one-to-many group chat by using tools such as instant messengers,

Internet Relay
Chat (IRC) etc.

**27. Electronic commerce**, commonly written as **e-commerce**, is the trading or facilitation of trading in products or services using computer networks, such as the Internet.

**28. Commercial transactions conducted electronically on the Internet.**

- Online shopping.
- Online market places.
- Business to business buying & selling.
- Online newsletter for marketing prospective.

**dedicated website** or other application which enables users to

**communicate** with each other by posting information, comments, messages, images , videos are referred to as social networks. For

example networks like

- Face book.
- Linked in.
- Twitter.

30. Due to worldwide use of computer network, people are now able to get together and form cyber communities that can **exchange messages** easily through cyberspace.
31. **Physically** meeting has been reduced due to introduction of cyber culture
32. **Culture** is an important process in computer related contexts.
33. Culture processes that **create meaning** in actions.
34. Cyber culture is indicated to break **down borders** and barriers, not only between nations but also between **groups and individuals**

Separated from each other due to some reasons.

35. If cyber culture grows then those who are cut off from **cyber culture** will feel more isolated from society and will not be properly updates about latest development and fast change.
36. The cyber culture has brought great impact on **human individual's life.** **37.**In education the style of teaching learning has changed The student teacher **interactivity** can be formed online.
38. The cyber culture has great influence in the **business world.**
39. The use of internet for emails and other social networks is our participation in the cyber culture
40. **Face to face** communication is becoming weak due to emerging of these social networks

41. The People who don't have the ability to communicate face to face they can exchange their views, through these **social network**.
42. Business decision can be made through **video Conferences**

43. All the dimensions **are physical** in nature

44. Perform all business transactions **off-line.**

45. Buy and sell products through physical **agents and representatives.**

46. All the dimensions are **digital** in nature.

47. **Pure online (virtual) organizations. Buy and sell products online.**

48. A combination of **physical and digital**

49. dimension

50. Primary business carried out in **the physical world**.

51. Provide some services **on line**.

52. **B2B Model describes commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a** retailer.

53. The **B2C model** involves transactions between business organizations and consumers. It applies to any business organization that sells its products or services to consumers over the Internet. These sites display product information in an online catalog and store it in a database.

54. The **B2C model** also includes services online banking, travel services, and health information.

Example: www.daraz.pk, www.amazon.com etc….

55. A **C2B model**, is a type of commerce where a consumer or end user provides a product or service to an organization

56. The **C2C model** involves transaction between consumers. Here, a

**consumer sells directly to another**

consumer. eBay.com, olx.com, etc…

57. A consumer uses **Web browser** to connect to the home page of a merchant's Web site on the Internet.
58. The consumer browses the **catalog** of products featured on the site and selects items to purchase.
59. The selected items are placed in the electronic equivalent of a **shopping cart**.
60. **When the consumer is ready to complete the purchase of selected items, He/she provides a bill-to and ship-to address for purchase and delivery.**
61. When the payment method is identified and the order is completed at the Commerce Server site, the merchant's site displays a **receipt** confirming the customer's purchase.

62. The Commerce Server site then forwards the order to a Processing Network for payment processing and **fulfilment**

63. Never send your **credit card** number to any site that is not secured.
64. Avoid sending any **photograph** online particularly to strangers.
65. Do not open mails from **strangers.** This prevents your system from unwanted attacks.
66. Don't respond to **harassing or negative** messages.
67. Learn more about **Internet** privacy.

68. Keep your operating system **up to date**.

**69.Change passwords frequently and Use hard-to- guess passwords.**

70. Don't share access to your computers with **strangers**.

71. If you have a Wi-Fi network, password **protect** it.

**72. Disconnect from the Internet when not in use.**

**73. Some of the possible prevention measures. One can take to avoid getting**

**victimized** for a cyber-crime

**74. Virus and Worms is a "program" that is loaded onto your computer without your knowledge and runs against your wishes**

75. **Hackers** A person who secretly gets access to a computer system in order to get information, cause damage, etc.

**76.**Hackers attack where they see **weakness**

**77. The word "malware" comes from the term "Malicious software."**

78. **Malware** is any software that infects and damages a computer system without the owner's knowledge or permission.

79.Download an **anti-malware** program that also helps prevent infections

80. **Trojan horses** are email viruses that can duplicate themselves, steal information, or harm the computer system.

81.**Trojan horses** viruses are the most serious threats to computers

**82. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.**

83. **Password attacks** are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites

84. Do not download **unfamiliar** software off the Internet

**85. The method of hiding plaintext in such a way as to hide its substance is called encryption.**

**86.** Encrypting plaintext results in unreadable gibberish called **cipher text**

87. **CA** is authorized to issue certificates to its computer users. (ACA's role is analogous to a country's government's Passport Office.)

88. The term "**Cyber Law"** Refers to all the legal and regulatory aspects of the Internet and its users

89. The **1st** rule of management is delegation. Don't try and do everything yourself because you can't.

**90. Cyber regulation 's evolution**

UNCITRAL 1966

- Model Law on
  - **E-Commerce 1996**
  - E-Signatures 1996
- Wipo Copy Rights Rules 1996
- Wipo Performance and Phonograms Treaty Rules 1996

**ICANN Uniform Domain Name Disputes Resolution Policy 1998**

\DMCA 1998

- UCD 2001
- ITA 2000
- The Electronic Transaction Ordinance
- 2002 Prevention of Electronic Crime Ordinance 2008

91. There are different laws, **promulgated** in Pakistan.

**92. These laws not only deal with crime of Internet**

93. These laws deal with all **dimensions** related to computer & networks.

94. **Two** of them are most known. They are:

- Electronic Transaction Ordinance 2002
  - Electronic / Cyber Crime Bill 2007 **23. 95.** There are **43** sections in this ordinance

**95. . Spamming is Illegal electronic messages to any person without the permission of the recipient**

96. There are seemingly **21 'cyber' issues** covered in this Bill

**97. The FIA, has been given complete and unrestricted control to arrest and confiscate material as they**

98. The Government has literally attempted to insert a new word in the **English** language eel necessary

**99. . The word TERRORISTIC is without doubt a figment of their imagination vocabulary**

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

101. The term "**Cyber Law"** Refers to all the legal and regulatory aspects of the **Internet** and its users

**102.** A hacker changed the value of insulin in a patient's online prescription who was admitted in a hospital the nurse injected that quantity and patient expired. **Cyber Murder**

103. _____penetrates into every corner of the modern business. Answer: E-commerce

**104.** The_____ rule of management is _____
Answer: **1st, delegation**

**105. Cyber regulation's evolution Table for remember:**

UNCITRAL **1966**

Model Law on
E-Commerce **1996**

E-Signatures **1996**

Wipo Copy Rights Rules **1996**

Wipo Performance and Phonograms Treaty Rules **1996**

ICANN Uniform Domain Name Disputes Resolution Policy **1998**

DMCA **1998**

EUCD **2001**

ITA **2000**

**106.** The Electronic Transaction Ordinance **2002**
**107.** Prevention of Electronic Crime Ordinance answer: **2008**
**108.** The rule of law and lawyer are Answer: **Consultancy**
109. The Subject matter Expert
**110.** A blend of Law and Technology **All of above**
111. The term "Cyber Law" Refers to all the legal and regulatory aspects of the Internet and its users
Answer: cyber law, internet ✓

112. A hacker changed the value of insulin in a patient's online prescription who was admitted in a hospital the nurse injected that quantity and patient expired. Answer: Cyber Murder ✓

113. _____penetrates into every corner of the modern business. Answer: E-commerce ✓

114. The_____ rule of management is _____
Answer: 1st, delegation ✓

115. Cyber regulation's evolution Table for remember:

UNCITRAL 1966 ✅

116. Model Law on E-Commerce 1996 ✅

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

ans:- jurisdiction

118. The right, power, or authority to administer justice by hearing ----------
-----
-?

ans:- Determining controversies.

119. Which is not a type of jurisdiction?
a) Territorial Jurisdiction
**b)** Extra Territorial Jurisdiction
**c) celluer jurisdiction**
d) Cyber Jurisdiction

120. ----------Refers-over cases arising in or involving ------ within a defined territory?

answer:-Territorial jursidictio & persons residing

121. which of the following is true about Extra territorail jursidiction?
a) jurisdiction over cases arising in or involving persons residing within a definedterritory.

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

c)**s to a court's ability to exercise power beyond its territorial limits.** d)Beyond the boundaries of nation statesenforcement of cyber laws uniformly accepted.

122. which one is virtual approach of jursidiction beyond states boundaries?

ans**:- Cyber jurisdiction**

123. what is cyber conflict?

ans:-A tense situation between nation-statesorganized groups where unwelcome cyber attacks may result in retaliation

124. what is the difference between cyber dispute and cyber attack or conflict??

ans:- **Both are same**

125. The Electronic Transaction Ordinance __

Answer: 2002 ✓

**126.** Prevention of Electronic

Crime Ordinance answer: **2008**

✓

127. The rule of law and lawyer
are Answer:
. Consultancy

128. Cyber security refers to the **technologies** and **processes** designed to protect computers, networks and data from unauthorized access and attacks delivered through the Internet by cyber criminals.
129. **Protecting** computer system and information from unauthorized access or destruction / abuse.
130. Security deal with three primary issues, called the **CIA** triad.
131. Confidentiality Assurance that only authorized user may access a resource.
132. Integrity Assurance that resources have not been modified.
133. **Availability** Assurance that authorized user may access a resource when requested.
134. Protecting information in the digital age requires **constant caution** to deter thieves who would steal financial, proprietary, and personal identification data.
135. Cyber security is necessary since it helps in **securing data** from threats such as data theft or misuse, also safeguards your system from **viruses**.
136. Security measures provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the **dynamic threats** posed by cyber thieves and cyber terrorists.
137. Your home computer is the popular **target** for intruders.
138. We can use our computers to **attack** other computers on the internet.
139. Intruder attacks home computer because it is not very **secure** and easy to
break into.
140. They do attack your computers by send us a E-mail with **virus**.
141. Trojan horses are such programs which are used as the **back doors**.

142. A Virus is a “**program**” that is loaded onto your computer without your knowledge and runs against your wishes.
**143.** Virus can reach to our computer through **CD-Rom.**
144. Virus can reach to our computer through **E – mail.**
**145.** Virus can reach to our computer through **Websites.**

146. Virus can reach to our computer through **download files**.
147. Install a security suite that protects the computer against threats such as viruses and worms.
148. Handle **E- mail** attachments carefully.
149. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
**150.** Hackers attack where they see **weakness.**
**151.** A system that hasn't been updated recently has flaws in it that can be taken advantage of by **hackers.**

152. Regularly **update** your operating system.
153. Install **Anti virus** software's.
154. The word "**malware"** comes from the term "Malicious software."
155. Malware is any software that infects and damages a computer system without the
156. owner's knowledge or permission.
157. Download an anti-malware program that also helps prevent infections.
158. Activate Network Threat Protection, Firewall, Antivirus.
159. **Trojan horses** are email viruses that can duplicate themselves,
160. steal information, or harm the computer system.
161. These viruses are the most serious threats to computers.
162. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
163. Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.
164. Protection against data from **theft**.
**165.** Protects the computer from being **hacked.**
166. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.
167. Crimes against a government are referred to as **cyber terrorism**.
168. In this category, criminals hack military
**169.** websites or circulate propaganda. **Cyber Crime Against Government**
**170.** There are categories of cyber-crime **3**
**171.** In this case, they can steal a person's bank details and misuse the credit card to make purchases online. **Cyber Crime Against Property**
172. Damaging or destroying data rather than stealing or misusing them is called
173.**cyber vandalism**.
174. ..... is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. **Cyber bullying**
175. ..... A criminal accesses data about a person's bank

**176.** account, credit cards, debit card and other sensitive information---.**Identity theft**
177. The software is used to gain access to a system to steal sensitive information or data or causing damage to software and hardware **Malicious Software**

178. _____The crime in which the attacker harasses or threaten

**179.** victim using electronic communication, such as e-mail, instant messaging (IM) ..**Cyber stalking**

**180.** _____This crime occurs when a person violates copyrights and unauthorized copying of software.
**Software Piracy**
**181.** _____in simple terms means illegal access into a Computer system without the permission of the computer owner/use. **Hacking**

182. There are types of cyber crime_____**numerous**.

## Lesson #1

## Introduction to Cyber Society, Cyber Culture and Cyber Space

**Cyber Society:** Focuses on the construction, maintenance and facilitation of community in electronic networks and computer mediated communication.

**Cyber Culture:**

- **Worldwide web** is the collection of electronic documents.
- Each electronic document on the web is called a web page which can contain text, graphics, audio and video.
- The use of World Wide Web by a people or a group of people for the exchange of social expectations, custom, history and language is called cyber culture.
- Like every culture has its own language, the cyber culture is not the exception to this rule.
- It converts the human written language or symbols to machine language and reconverts to human understandable language so the people on the destination can understand.
- Now a day's specially in online chatting the cyber language is creates of new codes which affects our daily spoken language.

## Cyber Culture Components

- Internet
- Website
- E-Mail
- Blog
- Online Chat
- E-Commerce
- Social Networks

## Cyber Culture Components

### Internet

1. The network formed by the co-operative interconnection of a large number of computer networks.
2. No one owns the Internet.
3. There is no central administration to the internet.
4. Main goal of the internet is to connect several computers together for the exchange of messages and share the information etc.
5. Community of people.
6. Collection of resources.

### Website

1) A location connected to the Internet that maintains one or more web pages.
2) Web pages are the building blocks of the website.
3) Web pages include documents like texts and multimedia contents etc.

4) A web site may be accessible through a public Internet Protocol (IP) network, such as the Internet, or a private local area network (LAN), by referencing a uniform resource locator (URL) that identifies the site.

**Email**

1) **Electronic mail**, most commonly called **email.**
2) E-mail is the most widely used application on the internet.
3) Messages that are sent electronically from one computer to another are an e-mail message.

**Blog**

1) A blogis a discussion or informational site published on the World Wide Web consisting of discrete entries ("posts").
2) A regularly updated website or web page, typically, runs by an individual or a small group.

**Online Chat**

1) Any kind of communication over the Internetthat offers a real-timetransmission of text messages from sender to receiver is calledonline chat.
2) Online chat may address point-to-point communications as well asmulticast communications from one sender to many receivers and video chat, or may be a feature of a web conferencing service.
3) Any direct text-based or video-based (webcams), one-on-one chat orone-to-many group chat by using tools such as instant messengers, Internet Relay Chat (IRC) etc.

## E-Commerce

- **Electronic commerce**, commonly written as **e-commerce**, is the trading or facilitation of trading in products or services using computer networks, such as the Internet.
- Commercial transactions conducted electronically on the Internet. E.g.
- Online shopping.
- Online market places.
- Business to business buying & selling.
- Online newsletter for marketing prospective.

## Social Networks

- A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images , videos are referred to as social networks. Forexample networks like
- Face book.
- Linked in.
- Twitter.

## Concept of Cyber Space

- The cyberspace is a term used to describe the space created through the union of electronic communications networks such as the internet, which enables computer facilitated communication between any numbers of people who may geographically dispersed around the globe.

- Cyberspace is a public space where individuals can meet, exchange ideas, share information, provide social support, conduct business etc.
- The human interaction does not require physical connection to communicate, but is rather characterized by the interconnection of millions of people throughout the world through chat room, email, Face book etc.

**Cyber Space Communities**

- Due to worldwide use of computer network, people are now able to get together and form cyber communities that can exchange messages easily through cyberspace.
- Physically meeting has been reduced due to introduction of cyber culture.

**The Culture of Computing**

- Culture is an important process in computer related contexts. The processes that create meaning in actions.
- Cyber culture is indicated to break down borders and barriers, not only between nations but also between groups and individuals separated from each other due to some reasons.
- If cyber culture grows then those who are cut off from cyber culture will feel more isolated from society and will not be properly updates about latest development and fast change.

**Effects of Cyber Culture on Society**

- The cyber culture has brought great impact on human individual’s life.

- In education the style of teaching learning has changed. The student teacher interactivity can be formed online.
- The cyber culture has great influence in the business world.
- The use of internet for emails and other social networks is our participation in the cyber culture.
- Cyber culture reduced the gap between groups and individuals separated from each other due to some reasons.
- Now days there are many social networking sites like Face book, MySpace and Twitter, which all serve to provide links to many friends to maintain their relationship.
- These social networks are means of interactivity between people around world.
- Face to face communication is becoming weak due to emerging of these social networks.
- The People who don’t have the ability to communicate face to face they can exchange their views, through these social network.
- Business decision can be made through video conferences.

**Outcome**

- The cyber culture is developing and we need to know the values and believes of this culture.
- Cyber culture has great influence on human culture and in way new uniform global culture is developing.

**Lesson #2**

# FUNDAMENTALS OF E-COMMERENCE

## E-Commerce Basics

- Process of buying, selling or exchanging products, services and information through computer networks.
- It refers to the use of the Internet and the Web to manage business between and among organizations and individuals.

## Domains of E –commerce

1) Physical Domain
2) Digital Domain

## Traditional E- Commerce

- All the dimensions are physical in nature
- Perform all business transactions off-line.
- Buy and sell products through physical agents and representatives.

## Pure E- commerce

- All the dimensions are digital in nature.
- Pure online (virtual) organizations.
- Buy and sell products online.

## Hybrid Approach

- A combination of physical and digital dimensions
- Primary business carried out in the physical world.
- Provide some services on line.

## Types of E-Commerce Models

Four Major Domain on which E-Commerce Works

1) Business-to-Business (B2B) Model
2) Business-to-Consumer (B2C) Model
3) Consumer –to-Business (C2B) Model
4) Consumer-to-Consumer (C2C) Model

**Business-to-Business (B2B) Model**

- B2B Model describes commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.
- **Example**: Dell deals computers and other associated accessories online but it does not manufacture all those products. So, in govern to deal those products, first step is to purchases them from unlike businesses i.e. the producers of those products.

**Business-to-Consumer (B2C) Model**

The B2C model involves transactions between business organizations and consumers. It applies to any business organization that sells its products or services to consumers over the Internet. These sites display product information in an online catalog and store it in a database. The B2C model also includes services online banking, travel services, and health information.

Example: www.daraz.pk, www.amazon.com etc….

**Consumer-to-Business (C2B) Model**

- A C2B model is a type of commerce where a consumer or end user provides a product or service to an organization.
- An example is Priceline.com, where the customer names a product and the desired price, and Priceline tries to find a supplier to fulfill the stated need.

**Consumer-to-Consumer (C2C) Model**

- The C2C model involves transaction between consumers. Here, a consumer sells directly to another consumer.
- eBay.com, olx.com, etc… are common examples of online auction web sites that provide a consumer to

advertise and sell their products online to another consumer.

**Process of E-Commerce**

- A consumer uses Web browser to connect to the home page of a merchant's Web site on the Internet.
- The consumer browses the catalog of products featured on the site and selects items to purchase.
- The selected items are placed in the electronic equivalent of a shopping cart.
- When the consumer is ready to complete the purchase of selected items, He/she provides a bill-to and ship-to address for purchase and delivery.
- When the payment method is identified and the order is completed at the Commerce Server site, the merchant's site displays a receipt confirming the customer's purchase.
- The Commerce Server site then forwards the order to a Processing Network for payment processing and fulfillment.

**Advantages of E-Commerce**

1) Faster buying/selling procedure, as well as easy to find products.
2) Buying/selling 24/7.
3) You can shop anywhere in the world.
4) Low operational costs and better quality of services.
5) No need of physical company set-ups.
6) Easy to start and manage a business.
7) Customers can easily select products from different providers without moving around physically.
8) Communication improvement.

**Disadvantages of E-Commerce**

1) Unable to examine products personally.
2) Not everyone is connected to the Internet.
3) There is the possibility of credit card number theft.
4) Mechanical failures can cause unpredictable effects on the total processes.

**E-Shopping Safety Tips**

- **Check out sellers**: Conduct independent research before you buy from a seller you have never done business with. Some attackers try to trick you by creating malicious websites that appear real, so you should verify the site before supplying any information.
- **Make sure the site is genuine**: Before you enter your personal and financial information to make an online transaction, look for signs that the site is secure.
- **Protect your personal information**: Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.
- **Turn your computer off when you're finished shopping**: Many people leave their computers running and connected to the Internet all day and night. This gives scammers 24/7 access to your computer to install malware and commit cyber-crimes.

**Outcome**

Have the concepts and processes that comprise the technical infrastructure of e-commerce sites and be able to solve problems about online transactions.

# INTRODUCTION TO CYBER CRIMES

## Cyber Crime:

- Computer crime or cyber crime refers to any crime that involves a computer, Mobile and a network.
- Computer may be used as a weapon for crime or as a target.

**The Computer as a Target**: Using a computer to attack other computers.

**The computer as a weapon**: Using a computer to commit real world crimes.

## Cyber Criminals:

- Those who are doing crimes by using the computer as a target or an object.

## What is Cyber Crime? Simple Theory

- When you purchase a home it comes with a door and a lock. You always ensure that the door/lock exist and working properly. You may even purchase security systems.
- Likewise, Your Computer System is your home and security tools are your door/lock.
- So if someone breaches into your computer System, accesses all your personal accounts and tampers your data, is the criminal who is committing the crime.
- And committed crime is known as cyber-crime.

## Categories of Cyber Crimes

### Cyber Crime against Individual

- This type of cyber crime can be in the form of hacking, identity theft, cyber bullying, cyber stalking etc.

### Cyber Crime against Property

- Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing.
- In this case, they can steal a person's bank details and misuse the credit card to make purchases online.

**Cyber Crime against Government**

- Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism.
- In this category, criminals hack government websites, military websites or circulate propaganda.

**Types of Cyber Crimes**

There are numerous types. Some of which are:

1) **Hacking:** Hacking in simple terms means illegal access into a computer system without the permission of the computer owner/user.
2) **Software Piracy:** This crime occurs when a person violates copyrights and unauthorized copying of software.
3) **Cyber Stalking:** The crime in which the attacker harasses or threaten a victim using electronic communication, such as e-mail, instant messaging (IM), or messages posted to a Web site or on social networking sites.
4) **Malicious Software:** These are Internet-based software or programsthat are used to disrupt a network. The software is used to gain accessto a system to steal sensitive information or data or causing damage tosoftware and hardware. (Virus, worms, Trojan horse, web jacking, emailbombing etc).

5) **Identity Theft:** A criminal accesses data about a person's bankaccount, credit cards, debit card and other sensitive information.
6) **Cyber Bullying:** Cyber bullying is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. This could be done via, text messages or images,personal remarks posted online, hate speeches and posting falsestatements in order to humiliate or embarrass another person.
7) **Denial-of-service attack:** This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.
8) **E-mail Spamming & Spoofing**: Email spoofing refers to email that appears to have been originated from one source and it was actually sent from another source. Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.
9) **Computer Vandalism**: Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. These are program that attach themselves to a file and then circulate.

**Safety Tips**

- Use antivirus software's.
- Insert firewalls.
- Uninstall unnecessary software.
- Maintain backup.
- Never send your credit card number to any site that is not secured.

- Avoid sending any photograph online particularly to strangers.
- Do not open mails from strangers. This prevents your system from unwanted attacks.
- Don't respond to harassing or negative messages.
- Learn more about Internet privacy.
- Keep your operating system up to date.
- Change passwords frequently and Use hard-to-guess passwords.
- Don't share access to your computers with strangers.
- If you have a Wi-Fi network, password protects it.
- Disconnect from the Internet when not in use.

**Outcome**

As internet technology advances so does the threat of cyber crime. In times like these we must protect ourselves from cyber crime. Antivirus software, firewalls and security patches are just the beginning. Never open suspicious emails and only navigate to trusted sites.

**Lesson #4**

## Cyber Security

**What is Cyber Security?**

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access and attacks delivered through the Internet by cyber criminals.
- Protecting computer system and information from unauthorized access or destruction / abuse.

Security deal with three primary issues, called the CIA triad.

1) **Confidentiality**: Assurance that only authorized user may access a resource.
2) **Integrity**: Assurance that resources have not been modified.
3) **Availability:** Assurance that authorized user may access a resource when requested.

**Need of Cyber Security**

- Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
- Security measures provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the dynamic threats posed by cyber thieves and cyber terrorists.

**Home Computer Security**

- Your home computer is the popular target for intruders.
- They look for credit card numbers, bank account information.
- Use your computers to attack other computers on the internet.

**Why Intruder attack home computers?**

- Not very secure
- Easy to break into

**How do they attack your computers?**

- They send you E- mail with a virus
- They often install new programs that let them continue to use yourcomputer (Back door).
- Trojan horses are such programs which are used as the back doors.

**Major Security Problems and Solution**

- Virus and Worms
- Hacker
- Malware
- Trojan Horses
- Password Cracking

**Virus and Worms:**

A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.

**Virus can reach to your computer in many ways as:**

- CD- Rom
- E-mails
- Websites
- Downloaded Files

Check each of the above for viruses before using it.

**Solution:**

- Install a security suite that protects the computer against threats such as viruses and worms.
- Handle E- mail attachments carefully.

**Hackers:**

- A person who secretly gets access to a computer system in order to get information, cause damage, etc.
- Hackers attack where they see weakness. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.

**Solution:**

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.
- Regularly update your operating system
- Install Antivirus software's.

**Malware:**

- The word "malware" comes from the term "Malicious software."
- Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

**Solution:**

- Download an anti-malware program that also helps prevent infections.
- Activate Network Threat Protection, Firewall, and Antivirus.

**Trojan horse:**

- Trojan horses are email viruses thatcan duplicate themselves, steal information, or harm the computer system.

- These viruses are the most serious threats to computers.

**Solution:**

- Security suites, such as Avast Internet security, will prevent you from downloading Trojan Horses.

**Password Cracking:**

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

**Solution:**

- Use always Strong password.
- Never use same password for two different sites.

**Things to do for Protecting Computer (Security Measures)**

**1.** Use security software.
**2.** Maintain current software and updates.
**3.** Never share passwords.
**4.** Do not click random links.
**5.** Do not download unfamiliar software off the Internet.
**6.** Log out or lock your computer.
**7.** Remove unnecessary programs or services.
**8.** Frequently back up important documents and files.

**Advantages of Cyber Security**

1. Protects system against viruses, worms, spyware and other unwanted programs.
2. Protection against data from theft.
3. Protects the computer from being hacked.
4. Minimizes computer freezing and crashes.
5. Gives privacy to users.

**Outcome**

Improve the knowledge about cyber security and to overcome several security loopholes, also it helps to spread awareness among normal people about emerging security threats. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.

**Lesson #5**

# CRYPTOGRAPHY

## Introduction to Cryptography

- The method of hiding plaintext in such a way as to hide its substance is called encryption.
- Encrypting plaintext results in unreadable gibberish called cipher text.

## Origin

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

## Caesar’s Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC where D=A, E=B, F=C, and so on. “SECRET” encrypts as “VHFUHW.

## Conventional Cryptography

It is very fast. It is especially useful forencrypting data that is not going anywhere.

**Key Management**

- Both ends must agree upon a key and keep it secret between them.
- Being on different physical locations, they must trust a courier (secure communication medium) to prevent the disclosure of the secret key.
- Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.

**Certificate Management and Distribution**

- Public Key Infrastructures
- Certification Authority, or CA
- CA is authorized to issue certificates to itscomputer users. (ACA's role is analogous to acountry's government's Passport Office.)

**Lesson #6**

## INTRODUCTION TO CYBER LAW

**Definition:**

The term "Cyber Law" Refers to all the legal and regulatory aspects of the Internet and its users.

**Cyber Murder**

A hacker changed the value of insulin in a patient's online prescription who was admitted in a hospital the nurse injected that quantity and patient expired.

**Need of Cyber Law**

- E-commerce penetrates into every corner of the modern business

- Regulatory Issues
- Emails
- Social Media
- Video Streaming
- Email spoofing
- Financial crimes
- Online gambling
- Sale of illegal articles
- Forgery
- Cyber Defamation
- Cyber stalking
- Denial of Service attack
- Trojan attacks
- Worms and Viruses
- Data diddling
- Intellectual Property crimes
- Cyber Disputes
- Unauthorized access to computer systems
- Salami attacks

**The role of Law and Lawyers**

- The 1st rule of management is delegation. Don’t try and do everything yourself because you can't.
- Consultancy
- The Subject matter Expert
- A blend of Law and Technology

**Cyber Regulation’s Evaluation**

- UNCITRAL 1966
- **Model Law on**
- E-Commerce 1996

- E-Signatures 1996
- Wipo Copy Rights Rules 1996
- Wipo Performance and Phonograms Treaty Rules 1996
- ICANN Uniform Domain Name Disputes Resolution Policy 1998
- DMCA 1998
- EUCD 2001
- ITA 2000

**Cyber Regulations in Pakistan**

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

**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:
- Electronic Transaction Ordinance 2002
- Electronic / Cyber Crime Bill 2007

## Electronic Transaction Ordinance 2002

### 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

- 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 InvestigationAgency (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 deviatingfrom 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**

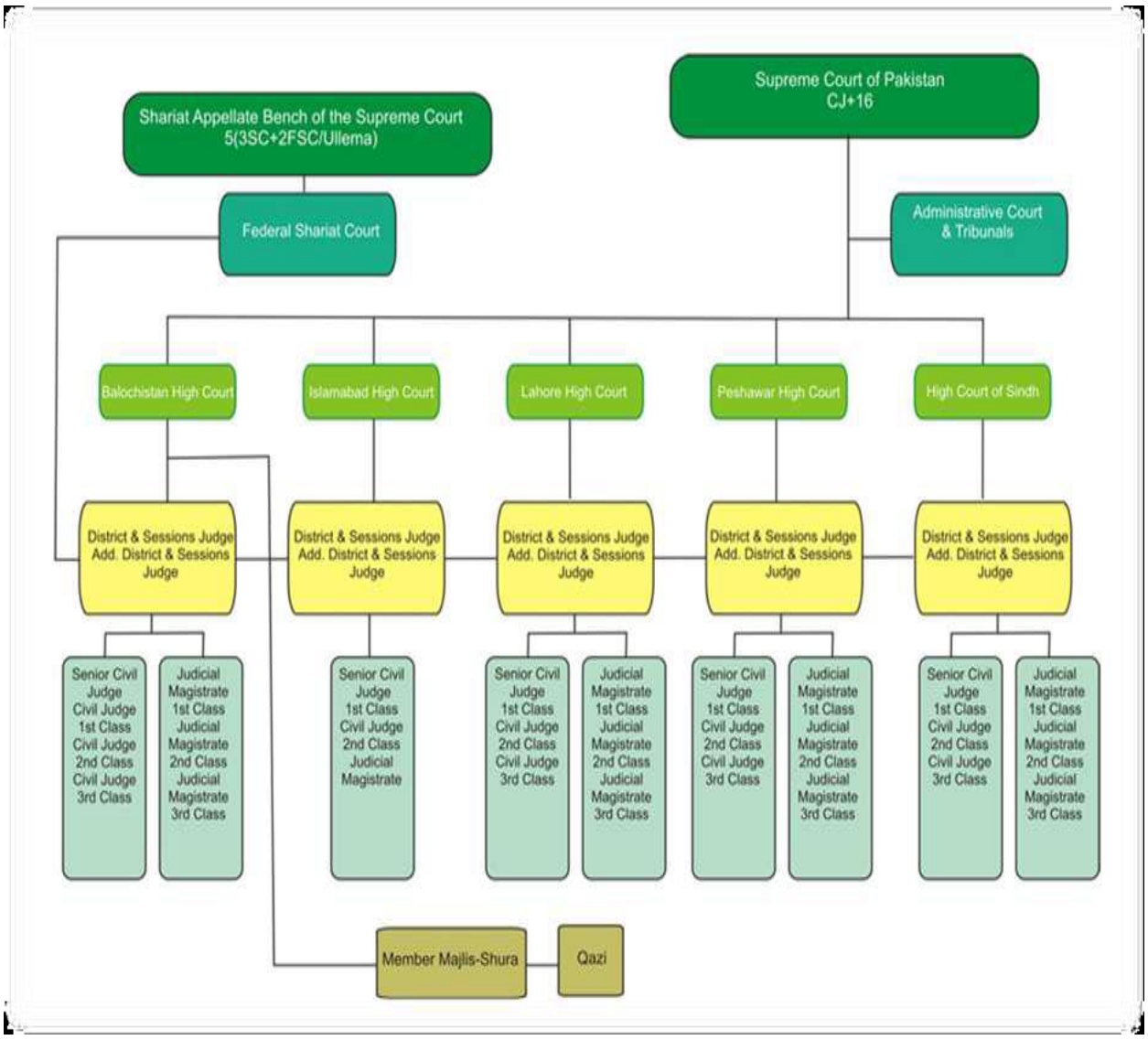
It refers to jurisdiction over cases arising in or involving persons residing within a defined territory.

**Extra Territorial Jurisdiction**

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 controlsrivalrous code, nobody else does. For example, no one but the ownerof an internet address (or those the owner permits) can post contentto that address. If person A owns a given internet address, person Bcannot put her website up at that address. If one person has a givenemail 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**

- 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**

- 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

- 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:**

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**

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 and6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).
- Any person who contravenes the provisions of this section shall be punished withimprisonment for a term which may extend to six months or with fine which mayextend 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**

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**

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**

- Punishment of Imprisonment
- Fine
- Compensation To Victim

## Lesson #12

## PREVENTION MEASURES FOR CYBER CRIMES

**Cyber Crime Cases**

- 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**

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**

Awareness learning needs to enter the 21st Century

- 49%Intentional attack by external hackers, criminals, terrorists or activists.

- 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.
- 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**

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**

Cyber censorshipis 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, predatorsPK, 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

# PROSPECTIVE

## What is a gTLD?

- 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 gTLDswere also selected by ICANN (theInternet Corporation for Assigned Names and Numbers) on November 16, 2000.

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 givencountry will be the most appropriate to hear and determine a case that hasan international dimension.
- A dispute has an international dimension where, for example, the partieshave different nationalities or are not resident in the same country.
- In such a situation the courts of several countries might have jurisdictionin 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 tothe 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 bothCivil 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**

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.