



ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

LESSON # 10

LECTURE OVER VIEW

- Establishment of Investigation and Prosecution Agencies
- National Réponse Centre for Cyber Crimes (Nr3c)
- Power of Officers
- Real Time Collection of Traffic Data
- Retention of Traffic Data
- Trans Order Access
- Warrant for Disclosure of Data



ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

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)

NATIONAL RESPONSE CENTRE FOR CYBER CRIMES (NR3C)

Responsabilités

Some of the responsabilités 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

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.

Contd..

- ❖ 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

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

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 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).
- ❖ Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to or with both.



WARRANT FOR DISCLOSURE OF DATA

WARRANT FOR DISCLOSURE OF DATA

The policy for warrant for disclosure of data Under Pakistan Electronic Crime act 2015 are 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.
- 

THANK YOU