Mapping Digital Crimes with Cyber Acts

Crime mapping is done by analysts in law enforcement agencies to map, visualize, and analyze and correlate data sources to create a detailed picture of crime incidents and related factors within a community or other geo-graphical area. It is a key component of crime analysis and the CompStat (a combination of management, philosophy, and organizational management tools for police departments) policing strategy.

Well, recent surveys have found that the use of computerized crime mapping is not widespread at this time, but the interest among law enforcement agency executives and planners appears to be growing for efficient & smart crime mapping techniques. The technology's efficiency continues to improve; and access to digital calls-for-service, arrest, and incident data within police departments is increasing. Digital crime mapping allows law enforcement agencies to plot crime-related data against a digitized map of a community, city, or region. Crime-related data then can be compared and analyzed with other external data sources. For digital crime mapping, one needs to have the raw data from various external sources like census data, city planning data, parks information,property assessment data, utilities information, and other data sources in conjunction with their crime data.

Why is there a need for mapping of Cyber crimes?

- To inform crime reduction initiatives.
- To enhance local and national responses.
- To identify gaps in response.
- To provide intelligence and risk assessment.
- To identify preventative measures.
- To facilitate reporting.
- To educate and inform the public.
- To identify areas for further research (identifying the requirements and a space to develop and apply new tools & technologies).

What includes in Cyber or Digital crimes?

- Basically the crimes including cyberspace & technologies.
- Use of computers to assist ‘traditional’ offending, either within particular systems or across global networks.
- Email Spamming.
- Ransomware, Malware attacks.
- Trojans, viruses.
- Crimes for economic gain (such as fraud, identity theft or blackmail).
- Cyberterrorism.
- Distribution of obscene contents.
- spreading hate and inciting terrorism.
- distributing child pornography, and many more.

To map & deal with digital crimes or cyber crimes, in India an act is introduced known as The Information Technology Act (IT Act), 2000. It consists of the different punishments & penalties for different kinds of digital offences.

1. **Tampering with computer source documents**

   Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter computer source docs shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

2. **Computer related offences** (Section 66)

   Dishonesty, fraudulency

3. **Sending offensive messages through communication service** (Section 66 A)

   Any information that is grossly offensive or has menacing character, causing annoyance or inconvenience, danger, obstruction, insult, hatred, ill will. Through any mailing or messaging services. Previously, punishable with imprisonment for a term which may extend to three years and with fine. But it has been removed now.

4. **Dishonestly receiving stolen computer resources or communication devices** (Section 66 B)

   Whoever dishonestly receives or retains any stolen computer resource or communication device will be believed the same to be stolen computer resource or communication device.

5. **Identity theft** (Section 66 C)

   Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person.

6. **Cheating by personation by using computer resource** (Section 66 D)
7. **Violation of privacy** (Section 66E)

   Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment.

8. **Cyber Terrorism** (Section 66F)
   - with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people
   - knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access
9. **Publishing or transmitting obscene material in electronic form** (Section 67)
10. **Publishing or transmitting of material containing sexually explicit act, etc., in electronic form** (Section 67A)
11. **Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form** (Section 67B)
12. **Preservation and retention of information by intermediaries** (Section 67C)
13. **Power of Controller to give directions** (Section 68)

14. **Power to issue directions for interception or monitoring or decryption of any information through any computer resource** (Section 69)
15. **Power to issue directions for blocking for public access of any information through any computer resource** (Section 69 A)
16. **Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security** (Section 69 B)
17. **Protected system** (Section 70)

    Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

18. **National nodal agency** (Section 70 A)
19. **Indian Computer Emergency Response Team to serve as national agency for incident response** (Section 70 B)

Now further in the investigation, digital forensics is done which includes scanning & penetration tools, Disk imaging tools - software imaging, hardware imaging, image restoration tools, Imaging validation tools, hidden data recovery tools, Data extraction tools, decryption or password cracking tools, for network forensics - packet analysis, traffic analysis, traceback, etc., system firewall logs, intrusion detection logs and many more.

But there are some gaps in mapping & investigation of cyber crimes.

- Lack of tools that verify the data during the acquisition process.
- Lack of tools that collect volatile evidence.
- Lack of tools that collect data from active systems.
- With current tools, the investigator requires to have an intimate knowledge of operating system commands & directory structure.

- Lack of tools for operation on different operating systems - some are compatible with windows only whereas some are compatible with Linux/Unix systems.
- Lack of tools capable of viewing obscure file formats.
- Lack of tools/techniques for analysis of Distributed systems.
- Lack of tools to identify users of chat networks.

Thank you !