THE DARK FACE OF MODERN TECHNOLOGY - CYBER CRIME

Vaasawa Sharma[1]

1. Faculty of Law, Starex University, Gurugram

Abstract

Technology plays a major role in shaping the world. With the advancement of science and technology, the world has changed as a result of which the life of people has also changed gradually with the passage of time. With the advent of internet, everything is available on and everyone has free right to access to any kind of information. But is it a boon or a bane for us? As we know that everything has uses as well as misuses also. Similarly, internet has many uses but the cyber crimes which are taking a lead can't be ignored. Despite of the fact that internet has given us a medium to live a better life and to gain knowledge without being messed up in the huge libraries we can easily find out any kind of information without wasting our time. But some people has developed their another world, that is the world of crime. they have searched the way of misusing the technology and use it for their benefit or to satisfy their unnatural desires. Cyber crimes are the crimes or offences that are committed by a person electronically or using any electronic media. These are very serious kind of offences because it was not easy to find out the accused.

Introduction

Evolution of Cyber Crime

The cyber crime is evolved from Morris Worm to the ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

Years	Types of Attacks
1997	Cyber crimes and viruses initiated, that includes Morris Code worm and other.
2004	Malicious code, Torjan, Advanced worm etc
2007	Identifying thief, Phishing etc
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack, Cyber warfare etc.

Source:

Classification of Cyber Crime

1. Crime against individuals: these are the crimes that are committed against the individuals or a person or their property. These offences are-
   - **Cyber Stalking:** it is an act of following or stalking someone online or through electronic medium. When a person continuously approaches another person via emails, messages on any social networking sites like Facebook, Instagram etc. unnecessarily or with malafide intentions then such person is said to commit an offence of Cyber Stalking.
   - **Spoofing via E-mail:** it is an act of forging an email or changing the source of an email, believing it to be an authentic source from which a email is being sent meaning thereby, the sender changes the name of the source without the knowledge of the receiver.
   - **Spreading obscene material:** this offence is common with females and girls of young age. The photographs on the social media is morphed by the criminal and can be used for any unlawful purposes like posting them o pornography site.

- **Spamming:** this is also known as "Junk Email". In this, a spammer sends an e-mail to million of people at the same time to receive a response. The spammers use spam bots to create email distribution lists.
- **Cyber Defamation:** the reputation of an individual is injured via social networking site or any other electronic form so as to defame that person.
- **IRC (Internet Relay Chat) Crime:** in IRC, people chat with each other through a common platform or we can say that it is a kind of group chat. But sometimes it is used by the criminals for setting their targets. They use to win the confidence of people and then starts harassing them by blackmailing them to post their nude photographs on internet for extorting money. Or trapping them by alluring job offers which later found to be false. It also includes children who gets easily trapped by the cyber criminals.
- **Phishing:** in this type of crime or fraud the login information, passwords, details of ATM, bank count information or any other confidential information is being taken by the criminal by using some tactic.
- **Hacking:** it is very common type of internet crime that includes hacking of facebook account, hacking of email account etc. in this the information of the account is taken up by the defaulters and they obtain the command over that account.
- **Virus Dissemination:** it is the system by which a malicious software destroys the information stored in the victim's computer by disrupting its operation.
- **Identity Theft:** theft of identity is another kind of offence related to internet in which the identity of another person is stolen as a result of which the personal and confidential information is also being taken away by the hacker for making transactions and purchases.

2. **Cyber Crime against Property:** these includes vandalism of computers, Intellectual Property Crimes, online threating, trespassing online etc. Intellectual Property Crime includes:
   - **Software Piracy:** it is the strict infringement of copyright that is to say that it is the illegal copying of software which belongs to someone else.
   - **Copyright Infringement:** it is copying the work of another person without his knowledge and permission. Copy of music, work of literature, art etc. comes within the ambit of copyright infringement.
   - **Trademark Infringement:** it is the copying of other person's trademark illegally or unauthorisedly.

3. **Crime against Oragization:** it includes
   - Deleting, reading or altering the data without any permission to do so.
   - **DOS Attack:** in this the attacker jams the server so that the system cannot be used by the user. It is a technique of making the server corrupt and making it unfit to use.
   - **Email Bombing:** a large number of emails are being sent to the victim in order to jam to server.
   - **Salami Attack:** in this, the personal information such as the details of debit or credit card are being stolen by the attacker but only very small amount is taken by him. These crime are not reported because the victim is unaware of such theft as the amount is very less. In this way an attacker deduces a little amount from various accounts.

4. **Crime against Society:** it includes:
   - **Forgery:** in simple words, it is an offence of forging signature, false document etc.
   - **Web jacking:** in this, the fake website is being created by the attacker, and when aperson opens that website another link opens up which opens another page. These types of attacks are done to get entrance or to get access and controls the site of another.[1]

Cyber Offences under India Penal Code

There are many provisions in Indian Penal Code related to Cyber Offences. These are:

- S. 292 : Sale etc. of obscene books, etc. this states that

(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or

[1] https://www.government.nl/topics/cybercrime/forms-of-cybercrime

if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(2)Whoever –

(a) Sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, reduces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other Obscene object whatsoever, or

(b) Imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) Offers or attempts to do any act which is an offence under this section, Shall be punished [on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second Or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

- S. 294 IPC : Obscene acts and songs : whoever, to the annoyance of others:
  (a) Does any obscene act in any public place, or
  (b) Sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.
- Sec. 420 IPC : Bogus websites, cyber frauds : Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
- S. 463 IPC : Whoever makes any false documents or part of a document with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery. The act of spoofing an e-mails comes under this provision.
- S. 378 IPC : this section describes theft of movable or corporeal property. The theft of computer hardware or the theft of online data comes within in ambit of this section.
- S. 425 IPC : This section deals with mischief, it states that "whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief". That is to say, any damage to the system of computer and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.
- S. 507 IPC : Criminal intimidation by an anonymous communication, whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided under s. 506.

Cyber Crimes (State/UT-wise) – 2016-2018

S. No	State/UT	2016	2017	2018	Percentage Share of State/UT (2018)	Mid-Year Projected Population (in Lakhs) (2018)+	Rate of Total Cyber Crimes (2018)++
1	2	3	4	5	6	7	8
STATES:							
1	Andhra Pradesh	616	931	1207	4.4	520.3	2.3
2	Arunachal Pradesh	4	1	7	0.0	14.9	0.5
3	Assam	696	1120	2022	7.4	340.4	5.9
4	Bihar	309	433	374	1.4	1183.3	0.3
5	Chhattisgarh	90	171	139	0.5	284.7	0.5
6	Goa	31	13	29	0.1	15.3	1.9
7	Gujarat	362	458	702	2.6	673.2	1.0
8	Haryana	401	504	418	1.5	284.0	1.5
9	Himachal Pradesh	31	56	69	0.3	72.7	0.9
10	Jammu & Kashmir	28	63	73	0.3	134.3	0.5
11	Jharkhand	259	720	930	3.4	370.5	2.5
12	Karnataka	1101	3174	5839	21.4	654.5	8.9
13	Kerala	283	320	340	1.2	350.0	1.0
14	Madhya Pradesh	258	490	740	2.7	814.7	0.9
15	Maharashtra	2380	3604	3511	12.9	1213.9	2.9
16	Manipur	11	74	29	0.1	30.8	0.9
17	Meghalaya	39	39	74	0.3	32.0	2.3
18	Mizoram	1	10	6	0.0	11.8	0.5
19	Nagaland	2	0	2	0.0	21.3	0.1
20	Odisha	317	824	843	3.1	435.5	1.9
21	Punjab	102	176	239	0.9	297.0	0.8
22	Rajasthan	941	1304	1104	4.1	765.9	1.4
23	Sikkim	1	1	1	0.0	6.6	0.2
24	Tamil Nadu	144	228	295	1.1	754.6	0.4
25	Telangana	593	1209	1205	4.4	370.3	3.3
26	Tripura	8	7	20	0.1	39.6	0.5
27	Uttar Pradesh	2639	4971	6280	23.0	2230.0	2.8
28	Uttarakhand	62	124	171	0.6	110.6	1.5
29	West Bengal	478	568	335	1.2	965.0	0.3
	TOTAL STATE(S)	12187	21593	27004	99.1	12997.9	2.1
UNION TERRITORIES:							
30	A & N Islands	3	3	7	0.0	4.0	1.8
31	Chandigarh	26	32	30	0.1	11.7	2.6
32	D&N Haveli	1	1	0	0.0	5.3	0.0
33	Daman & Diu	0	0	0	0.0	4.0	0.0
34	Delhi UT	98	162	189	0.7	195.6	1.0
35	Lakshadweep	0	0	4	0.0	0.7	6.0
36	Puducherry	2	3	14	0.1	14.8	0.9
	TOTAL UT(S)	130	203	244	0.9	236.0	1.0
	TOTAL (ALL INDIA)	12317	21796	27248	100.0	13233.8	2.1

Note : i) '++ Crime Rate is calculated as Crime per one lakh of population.

TABLE 9A.1 Page 1 of 1

ii) '+ Population Source: Technical group on Population Projections Nov,2019 National Commission on Population, MoHFW based on 2011 census.

iii) As per data provided by States/UTs

iv) Clarifications are pending from West Bengal, Assam, Arunachal Pradesh, Meghalaya & Sikkim

Information Technology Act, 2000

The Information Technology Act came into force on 17 October 2000. It is the first law which was formed to deal with electronic commerce and online offences. It extends to whole of the India including the State of Jammu and Kashmir and it provides extra-terriorial jurisdiction.

Non- Applicability of the Act:

As per s. 1 (4) of the Information Technology Act, 2000, nothing in the act shall apply to-

(a) Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
(b) Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
(c) Creation of Trust under the Indian Trust Act, 1882.
(d) Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
(e) Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
(f) Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

Offences under the Act

- **Tampering with computer source documents:** Under s. 65 of this Act Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer Programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both. It is tried by any Magistrate and is cognizable and non-bailable offence.
- **Hacking with computer system:** S. 66 provides that- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

It includes receiving stolen computer or communication device, using passwords of another person, cheating using computer resource, publishing private images of others, act of cyber terrorism under sections 66 B, 66C,66D, 66E, 66F respectively.

- **Publishing of obscene information in electronic form:** S. 67 of this Act provides that Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. Under section 67A the punishment for publishing images containing sexual explicit acts or conduct and under section 67 B, punishment for an offence, if a person captures, publishes or transmits images of a child in a sexually explicit act or conduct or if a person induces any child to perform any sexual act. A child here means under the age of eighteen years. Then such person is liable for imprisonment upto five years and or with fine of rs.1,00,000 on first conviction and imprisonment upto seven years and or fine of rs. 1,000,000 on second and subsequent conviction.
- **Publication for fraudulent purpose:** S. 74 provides that- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extends to one lakh rupees, or with both.

Relevant Case Laws

1. **Sony Sambandh.com**

It was the first conviction under Cyber Law which came into light in 2013. The complaint was filed by Sony India, which had a website in the domain name of www.sony-sambandh.com, it was alleged that they were targeting Non-Residential Indians. The said website enabled the NRIs to extend Sony Products to their friends and relatives in India after the online payment is made by them. In May 2002, someone logged into the website which was in the name of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. All the transactions were being processed by the Credit Card and the request was made to deliver the products to Arif Azim in Noida. The delivery was made as desired. The digital photographs were also been aken by the company. But after one and a half month the credit card agency intimated the company that the transaction was an unauthorized one. The company lodged the complaint under s. 418, 419 and 420 of IPC to Central Bureau of Investigation. After due interrogation Arif Azim was arrested. Then he revealed that he worked in a call centre in Noida, where he gained an

access to the credit card number of an American National. The court took the lenient view because the boy was only 24 year old, the conviction was made accordingly.[2]

2. The Bank NSP Case

It was one of the leading case in Cyber Law. There was a management trainee of the bank, she was engaged to be married. The couple used to communicate via emails using the computer of the company. But after sometime they broke up with each other and he girl started sending fraudulent emails to foreign clients, due to which the boy's company lost their clients. The bank was held liable for the emails sent using the bank's system.

3. SMC Pneumatics (India) Pvt. Ltd. V. Jogesh Kwatra

It is the case of cyber defamation where the High Court of Delhi passed an ex-parte injunction. In this case the defendant Jogesh Kwatra was the employee of the company of plaintiff Mr. R.K. Malhotra. The defendant started sending defamatory, obscene, vulgar emails to the employers and also to the different subsidiaries all over the world just to defame the plaintiff reputation. The suit ws filed by the plaintiff for permanent injunction to restrict the defendant from further sending the derogatory, obscene, humiliating and defamatory emails to its sister subsidiaries. After going through the detailed arguments the Hon'ble Judge of High Court held that it is a case of cyber defamation and granted ex-parte ad interim injunction.[3]

4. State of Tamil Nadu v. Suhas Katti

This case was a remarkable judgement which took the time of just 7 months from the date of filing of an FIR. The victim was a divorced woman who was being mentally harassed by the accused. He opened a fake account of her name and used to send vulgar and obscene messages to her on Yahoo messenger group. This resulted in fake phone calls and disturbing messages. She filed a complaint in February 2004 and in the next few days the accused was arrested. He was a family friend of the victim who proposed her for marriage which she denied. The case was filed under section 469, 509 of IPC and section 67 of IT Act, 2000.
The accused paid the fine amount, and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of the Information Technology Act 2000 in India.[4]

5. Poona Auto Anillaries Pvt. Ltd., Pune v. Punjab National Bank, HO, New Delhi and others

In this case, largest compensation awarded in legal adjudication of a cyber crime dispute, Maharashtra's IT secretary Rajesh Aggarwal had ordered PNB to pay Rs 45 lakh to the Complainant Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. A fraudster had transferred Rs 80.10 lakh from Matharu's account in PNB, Pune after Matharu responded to a phishing email. Complainant was asked to share the liability since he responded to the phishing mail but the Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the Complainant.[5]

6. Mphasis BPO Fraud:

This case was regarding opening of bank account by using fake identity.fur call center employees collected the data of clients fraudulently. They transferred funds to the new Indian Bank Accounts. By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000.

Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.[6]

[2] https://www.cyberralegalservices.com/detail-casestudies.php
[3] Ibid
[4] Ibid
[5] https://www.itlaw.in/judgements/
[6] https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

Conclusion

Cyber Crime is one of the world's heinous crimes that not only ruins the victim's life but also leaves the victim in mental agony. As the technology is taking lead day by day, the criminals are also finding ways to fulfil their malafide intentions. Cyber Crime is a developing crime and is also complicated to interrogate. Various steps are being taken to control these crimes Cyber Cells are also established to investigate into these matters. The most common crimes are computer hacking, identity theft, injecting viruses and worms etc. The technology needs some improvements so that there can be easy detection and prevention of such activities. Effective remedies are also requires to cope up with such crimes. More stringent laws are required to deal with cyber crime, more cyber security is required and more privacy needs to be made to protect the valuable data and other documents etc. More and more investigating agencies are also required to be made. Cyber Cells should be given wider powers and infrastructural facilities to catch the criminals. There is need to make advance technology, improved connectivity to reduce more cyber abuses. Certain safeguards also needs to be made and strict implementation of laws is required so that we can use safe and technology

References

Holt, T. J., and A. M. Bossler. 2016. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series*. New York: Routledge. [Google Scholar]

Holt, T. J., A. M. Bossler, and K. C. Seigfried-Spellar. 2018. *Cybercrime and Digital Forensics: An Introduction*. 2nd ed. New York: Routledge. [Google Scholar]

McGuire, M., and S. Dowling. 2013. "Cybercrime: A Review of the Evidence." Home Office Research Study. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf [Google Scholar]

Per Lord Havers in R v Sharp [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion 1981

Keane, Modern Law of Evidence, 2005, pages 246-266. 1982

Dennis, The Law of Evidence, 2002, Chapters 16-17.

Galves, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 242. 1983

Galves, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

D. Ariz. (April 19, 2000), American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99- 185 TUC ACM, 2000 U.S. Dist. Lexis 7299.

Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26. Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502_enron.html, Visited: 28/01/2012

Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.

Hoffer, J. A., and D. W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43