University Research Resource Journal
Jayoti Vidyapeeth Women's University, Jaipur
Volume – 4, Issue – 2 (April – June - 2021) Page No: 75-97

ISSN: 2581 - 3730

Need of Popularization of Cyber Security

Prof. Dr. S. Lal[1]

Department of Science and Technology,

Jyoti Vidyapeeth Women's University, Jaipur (Rajasthan) dr.

lalshobha@gmail.com

Ms. Raj Sinha[2]

Research Scholar

Department of Computer Science and Information Technology, Jyoti Vidyapeeth Women's University, Jaipur (Rajasthan) rajsinha2310@gmail.com

Idea originator: We are very thankful to **Dr. Pankaj Garg Sir** , for organising such conferences which highlights the social issues and issues in the works faced by women in present working situations.

Again presenting my gratitude by remembering the famous quote

"As we look ahead into the next century, leaders will be those who empower *others." – Bill Gates.*

Abstract: Incidence of cybercrime in India is increasing day by day. A fastest growing area Cyber Crime is defined as any illegal activity that uses a computer as its primary means of commissions. According to NCRB data after U.S.A and China, India ranked third in malicious activity. Need, Opportunity and Rationalization give birth to cybercrime. Threats of cybercrime involve financial loss, legal repercussion, disclosure of confidential information, Reputational damage, inability to deliver critical service, time wastage, etc. Cybercrime is classified on basis of legal prospective, nature of crime and other. Methods of cybercrime include Cyber Stalking, Domain Names, Cyber-Squatting, Cyber-Extortion, Cyber-Cheating, Cyber-Warfare, Cyber-Terrorism, Phishing and Vishing. Most popular methods are Cyber Stalking, Domain Names and Cyber Squatting. To prevent cybercrime GoI has launched National Cyber Security Policies in 2013. Cyber Crime in India are registered under three main head i.e., IT Act, The IPC (Indian Penal Code) and State Level Legislations (SLL).

Keyword: Legal prospective, Cyber Stalking, Cyber Squatting

Scope of future research: Cyber security is significant on the grounds that it includes everything that relates to ensuring our delicate data, actually recognizable data (PII), secured wellbeing data (PHI), individual data, licensed innovation, data, and administrative and industry data frameworks from robbery and harm endeavoured by crooks and enemies.

Cyber security chance is expanding, driven by worldwide network and utilization of cloud administrations, similar to Amazon Web Services, to store delicate data and individual data. Broad poor arrangement of cloud administrations combined with progressively advanced cyber crooks implies the hazard that your association experiences a fruitful cyber assault or data break is on the ascent. Cyber security's significance is on the ascent. In a general sense, our general public is more innovatively dependent than any other time in recent memory and there is no sign that this pattern will slow. Individual data that could bring about wholesale fraud is presently presented on general society on our internet based life accounts. Delicate data like government managed savings numbers, Mastercard data and financial balance

subtleties are currently put away in distributed storage administrations like Dropbox or Google Drive.

Research outcomes: The quick mechanical progressions like the web unmistakably take steps to abandon the law. The open and unregulated nature of the web and the insignificance of topography implies that the web likewise gives pointless ground to criminal endeavor. The current criminal law is by all accounts sick outfitted to manage this up-degree in techniques and media of carrying out wrongdoing. Cyber-wrongdoing has therefore become a reality in India, hard to recognize, only here and there detailed and even hard to demonstrate. PC related wrongdoing does not have a customary paper review, is away from regular policing and requires masters with a sound comprehension of PC innovation. Paperless agreements, advanced marks, online exchanges and cyber violations have shocked the lawful world. Customary laws defined to oversee the basic and less criminal world are moronic and toothless. Proof, the establishment stone of the incredible lawful structure endures shock. The greatest pass up absence of visual proof. The web lattice has upset the legitimate mood though the lawful arrangements are pursuing the cyber lawbreakers who are falling back on new usual way of doing things every so often.

The constitution of India ensures equivalent right to life, instruction, wellbeing, food and work to women yet a similar humility of women appears not to be secured when all is said in done in the Information Technology Act, 2000. There are no particular arrangement in the IT Act, 2000 that explicitly manage the wrongdoing against women as does the arrangements of the Indian Penal Code, the Constitution of India or the Code of Criminal Procedure so far as that is concerned.

In an ongoing turn of events, the administration established a specialist gathering to examine the holes and difficulties in taking care of cybercrimes and set up a guide for adequately handling cybercrimes and dependent on the groupâ€™s suggestions, the Cyber Crime against Women and Children (CCPWC) conspire has been endorsed by the legislature.

The meaningful arrangement of Section 77 of the IT Act gives that the arrangements of Indian Penal Code will in any case apply to all the conditions and that the punishment under any arrangement of the IT Act don't discharge the guilty party from the obligation under

some other law. Crimes which are particularly focused against women might be counted as cyber-following, cyber slander, cybersex, scattering of profane material and intruding into one€™s protection space is regular now-a-days.

The cyber erotic entertainment is basically characterized under area 66 An E, 67, 67A and 67

B. All erotic entertainment related offenses are bailable according to Section 77B of the Information Technology Act, 2000 the main special case being Section 67 An and 67B. This is the principle motivation behind why the guilty parties are submitting sex entertainment related offenses and still have the boldness to rehash it, as they are qualified for bail starting at right and also the long time for testing. These segments of the Act ought to be made non-billable in order to strike dread into the psyches of guilty parties, this will decrease the crime percentage to some extent.

Introduction: IT has become widespread and all-incredible in the lives of people and business over the globe. Mechanical headways in the territory of data and correspondence are developing at an extraordinary pace. It has changed the manner in which individuals think, act and react. Cyber implies something identified with PC or a PC system and wrongdoing alludes to a demonstration that is deserving of law and frequently against open request. Consequently, Cyber Crime alludes to any criminal behaviour or a wrongdoing that is carried out with the assistance of a PC, organize, electronic contraptions and hardware utilizing chip. In basic terms, a cyber wrongdoing is a wrongdoing where a PC is the instrument or the objective of the wrongdoing. Phishing, hacking, bypassing complex framework security systems, cyber following, card cloning and abusing encryption are a portion of the cyber violations submitted utilizing PC. They are getting steadily progressively famous utilizing cell phones, tablets, PDAs. POS, and so on

A critical piece of cybercrime is its nonlocal character: exercises can occur in wards secluded by enormous partitions. These stance significant issues for law approval since effectively close by or even national infringement by and by require worldwide cooperation. For example, if an individual gets the chance to kid suggestive amusement arranged on a PC in a country that doesn't blacklist kid sex diversion, is that individual executing a bad behaviour in a nation where such materials are unlawful? Where decisively does cybercrime occur? Cyberspace is basically an increasingly excessive type of the space where a telephone conversation occurs, some place near the two people having the conversation. As a planet-spreading over framework, the Internet offers culprits distinctive hiding spots as a general rule similarly as in the framework itself. Nevertheless, comparatively as individuals walking around the ground leave means that a skilled tracker can follow, cybercriminals leave snippets of data with respect to their character and region, notwithstanding their sincere endeavours to cover their tracks. In order to follow such snippets of data across national cut-off points, be that as it may, overall cybercrime plans must be confirmed. Cybercrime runs over a scope of activities. Toward one side are infringements that incorporate key breaks of individual or corporate assurance, for instance, ambushes on the dependability of data held in cutting edge safes and the use of improperly got electronic data to force a firm or individual. In like manner, at this completion of the range is the creating bad behaviour of data extortion. Most of the way along the range lie trade-based infringement, for instance, distortion, managing in youth sex diversion, modernized burglary, unlawful assessment shirking, and

copying. These are express bad behaviours with unequivocal losses, yet the criminal stows away in the relative mystery gave by the Internet.

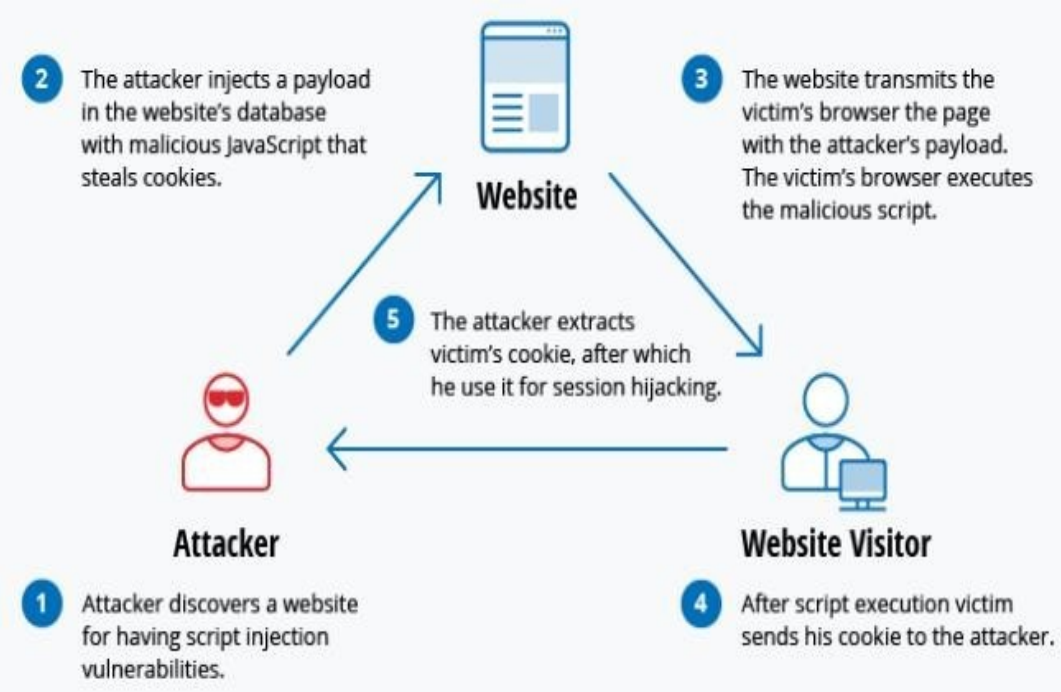


Fig 1.1. Process of Cyber Crime

Another bit of this sort of bad behaviour incorporates individuals inside ventures or government associations deliberately modifying data for either advantage or political goals. At the contrary completion of the range are those infringement that incorporate undertakings to upset the genuine activities of the Internet. These range from spam, hacking, and refusal of organization ambushes against express regions to exhibits of cyber terrorism—that is, the usage of the Internet to cause open aggravations and in any event, passing. Cyber terrorism focuses upon the use of the Internet by nonstate performers to impact a nation's money related and mechanical structure. Since the September 11 ambushes of 2001, open consideration regarding the peril of cyber terrorism has grown fundamentally.

There has been a basic addition in cybercrime against women, especially sextortion, during the COVID-19-provoked lockdown with "restricted gangsters" concentrating on them on the web, say experts.

The nation over lockdown constrained from March 25 to April 14, by then contacted May 3, and again loosened up to May 15, targets thwarting the spread of the novel coronavirus that has affirmed 1,147 lives and polluted 35,043 people in the country.

According to National Commission for Women (NCW) data, 54 cybercrime complaints were gotten online in April interestingly with 37 grumblings - jumped on the web and by post - in March, and 21 protests in February. The board is taking fights online due to the lockdown.

Methods of Cyber Crime: Following are different methods of cyber crime

- Cyber-Stalking
- Domain Names
- Cyber-Squatting
- Cyber-Extortion
- Cyber-Cheating
- Cyber-Warfare
- Cyber-Terrorism
- Phishing and Vishing

Some of the common methods of Cyber Crime are explained below:

Cyber Stalking: Alludes to PC arranged badgering, online provocation or online maltreatment is a gathering of conduct, for example, fraud, information burglary, harm to information or gear, PC observing, the requesting of minors for sexual purposes and

encounter wherein an individual, gathering of people or association utilizes data and interchanges innovation to disturb at least one people.

Fig 1.2. Cyber Stalking

Types of Cyber Stalking:

- Email Stalking
- Internet Stalking
- Security Stalking

Causes of Cyber Stalking

- Harassment
- Fascination
- Revenge
- Boasting

Methods of Cyber Stalking: Follow online activities of Victim

Legal Recognition:

Section 354D deals with stalking of women.

Information technology act 2000:

- Section 67 of the Act
- Section 43 A
- Section 500 of the Indian Penal Code

The criminal law (Amendment) act 2013:

- Section 35D of the IPC(Indian penal code)

Challenges of Cyber Stalking:

- No Provision for stalking of Men
- Separate stalking law is missing
- Immediate action from police department is missing which resulted in the suicide of Vinupriya
- IT Act 2000 has no specific provision for cyber stalking

Prevention of Cyber Stalking:

- Review your privacy settings on social media sites.
- Don't share real details of activity in FB account
- Avoid revealing Real Time Information such as exact location
- Set Strong and unique password.
- If possible enable 2 factor authentications to get more secure communication
- Use VPN Service when sending private emails or sharing sensitive information when connected to an unsecured public Wi-Fi
- Sensitive Information should not be disclosed
- Maintain good digital hygiene
- Hide IP Address with VPN
- Keep software up to date
- Keep low profile to avoid
- As soon as you begin to receive threats report in police department.
- Keep a copy of online image or messages as threat

Domain Names: It is a unique name that identifies a website in the network. Every website has IP address that identifies network of the computer system and uses it for access as part of the particular protocol for transmission of the data packets.

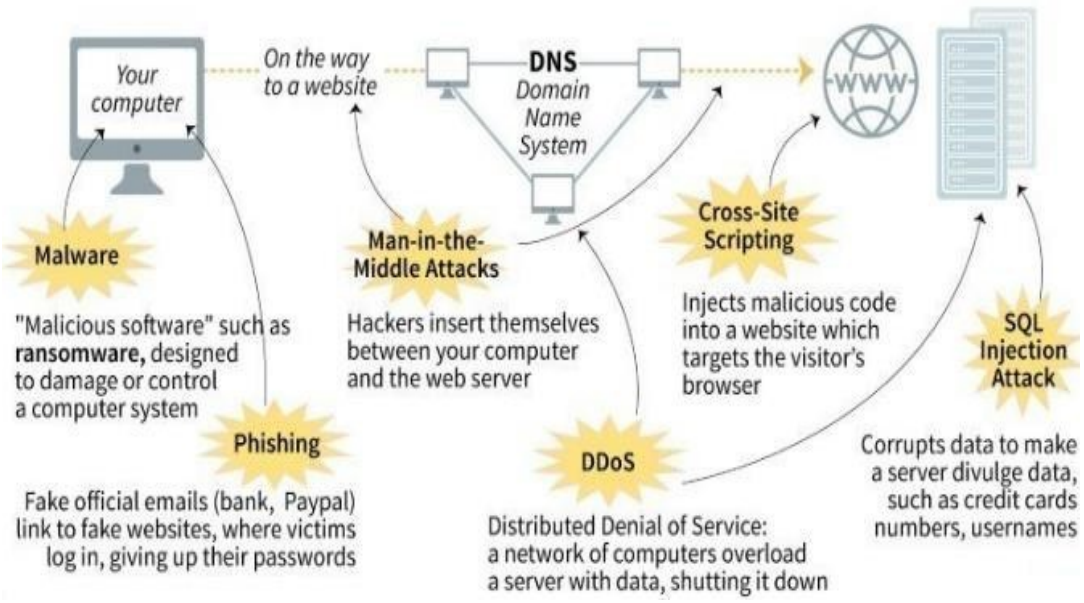


Fig 1.3. Cyber Crime through DNS

For Eg: www.anytrademarkname.com.in

Here, www.-Site is linked to World Wide Web

anytrademarkname.- Pick and in a perfect world perceives association name or center business

Below table shows some domains description:

Domains	Description
.com	show organization is occupied with business movement
.in	Company is registered in India

Table 1.0: Domain Description

Cyber Squatting: Squatting means sitting or bending down to occupy a space. Also known as Domain Squatting, is a common method to infringe a trade mark by using internet domain name or registering a domain with an illegal intention to use someone else business or trade

mark to make profit. In straightforward terms, Cybersquatting is the act of enrolling brand names of presumed organizations as Internet areas for the goal of selling them later at a benefit.

Fig 1.4. Cyber Squatting

Types of Cyber Squatting:

- Criminal Cybersquatting
- Protective Domain squatting
- Unintentional Domain squatting.
- Typosquatting
- Gripe Sites

Causes of Cyber Squatting:

- Make profit from others
- Damage to brand name
- Use the domain name to attract traffic and generate money through advertising

Methods of Cyber Squatting:

- Register brand names of Reputed Companies
- infringe a trade mark by using internet domain name

Legal Recognition:

- Anti-cybersquatting Consumer Protection Act(ACPA)
- Challenges of Cyber Squatting:
- IT law of India has not addressed the issue of domain name protection.
- Copyright infringement issues
- Setup a brand monitoring system
    - SecurityTrails API
    - Domain Feeds
    - Surface Browser

Prevention of Cyber Squatting:

- Choose several top-level domains as per (ICANN)
- Infrastructure top-level domain (ARPA)
- Generic top-level domains (gtld)
- Restricted generic top-level domains (grtld)
- Sponsored top-level domains (stld)
- Country code top-level domains (cctld)
- Test top-level domains (ttld)
- Generic Top Level Domains (gtlds)
- Country-Code Top Level Domain (cctlds)
- Reserve domain name on priority basis
- Check your domain name on frequent basis
- Register domain name
- Monitor new domain registration
- Type the URL — and make sure it's totally accurate
- Don't open suspicious emails — or click links within them
- Eliminate vulnerabilities in your OS and applications
- Install Internet security software — and keep it updated

Review of literature: Mostly used as a prefix these days the word 'cyber' has got recent origin in the history. This word has acquired popularity as 'cybernetics' or the Greek word 'kybernetes'. However, it later acquired importance in its abbreviated form 'cyber' and then as a prefix in the word 'cyberpunk', 'cybertalk' and 'cyberspace'. The word 'Cyber' is often related to computer or computer network. The other words that are closely associated with cyber crimes are:

Online Frauds, E-Frauds, Network Frauds, Internet Frauds, Cyberspace fraud, remote access crimes, virtual world frauds, etc.

Reported Incident in the past:

Year	Incidence
1820s	First cyber security took place in France textile manufacture industry that produced loom.
1989	The WANK Worm hit NASA offices in Greenbelt, Marryland
1999	Small group of hackers from southern England gained control of a military satellite
2000	Maxim(Hacker) stole the credit card information by breaching CDUniverse.com
2006	Automated Apply Yourself surfaced with dozens of top business schools in order to track their application status including Harvard and Standford.
2008	26,000 Site Hack attack when MSNBC.com was among the largest 1000 of sites used by a group of unknown hacker earlier to redirect traffic to their own malware servers.

Table 1.1: Reported Incident in the Past

Mostly used as a prefix these days the word 'cyber' has got recent origin in the history. This word has acquired popularity as 'cybernetics' or the Greek word 'kybernetes'. However, it later acquired importance in its abbreviated form 'cyber' and then as a prefix in the word 'cyberpunk', 'cybertalk' and 'cyberspace'. The word 'Cyber' is often related to computer or computer network. The other words that are closely associated with cyber crimes are: Online

Frauds, E-Frauds, Network Frauds, Internet Frauds, Cyberspace fraud, remote access crimes, virtual world frauds, etc.

Manish Kathuria Case: First reported instance of digital crime:

Case	Description
Recorded a case	Ritu Kohli has been trailed by Kathuria on a talk site www.mirc.com that mishandled her by utilizing foul language and afterward scattered her phone number to different individuals. Finally, he started utilizing Kohli‟s personality to visit on this site.
Against	Ritu kohli who uses www.mirc.com to mishandled Kathuria site. Received right around 40 profane calls at odd hours of the night more than three sequential days
Result	Delhi Police followed the IP addresses and captured Kathuria under Section 509 of the Indian Penal Code. The IT Act was not summoned for the situation, since it had not come into power when the protest was documented.

Table 1.2: Manish Kathuria case

President Pranab mukharjee's daughter Sharmistha Mukherjee stalking case:

Case	Description
Recorded a case	Sharmistha Mukherjee was allegedly harassed by a man, who posted sexually explicit messages on her Facebook page
Result:	Sharmistha Mukherjee lodged a complaint with the Cyber Crime unit of Delhi Police. On investigation the messages were found to be sending from FB Messenger, the man is resident of Nauhati in Hooghly, West Bengal named Partha Mandal

Table 1.3: President Pranab mukharjee's daughter Sharmistha Mukherjee stalking case

Yahoo! Inc. vs. Akash Arora & Anr. (1999) : This is one of the soonest and critical digital hunching down case in India.

Case	Description
Recorded a case	Web internet searcher Yahoo (offended party)
Against	A digital vagrant (Akash Arora and Anr.)
Why?	Using the area name www.yahooindia.com Akash Arora and Anr. was professing to be an augmentation of Yahoo in India and was offering catalog administrations with data explicit to India.
Result	• The Delhi High Court allowed a directive against the digital vagrant • Trademark law applies with equivalent power on the Internet like the physical world.

Table 1.4: Yahoo! Inc. vs. Akash Arora & Anr. (1999)

Rediff Communication Ltd. versus Cyberbooth and Anr. (1999) :

Case	Description
Documented a case	Web crawler Rediff i.e., www.rediff.com
Against	A digital vagrant (Cyberbooth and Anr.)
Why?	Using the space name www.radiff.com

Result	Bombay High Court saw that space names is an important corporate resource, as it encourages correspondence with a client base. The court expressed that the likeness in site names can befuddle the general population, especially new clients.

Table 1.5: Rediff Communication Ltd. versus Cyberbooth and Anr. (1999)

googkle.com and ghoogle.com:

Case	Description
Documented a case	A Russian man made the sites googkle.com and ghoogle.com to embed malware on client machines.
Against	In 2011, Google documented a grievance with National Arbitration discussion and effectively got "Goggle.com", "Goggle.net", and "Goggle.org", which were considered phishing/extortion destinations, brought down.
Why?	googkle.com and ghoogle.com was being used by Russian man
Results	Google won the rights back to the spaces in 2005 "Goggle.com", "Goggle.net", and "Goggle.org" belongs to Google

Table 1.6: googkle.com and ghoogle.com

Material and methods: The Material and methods includes the methods for the collection of the data , in this paper we have collected the data from the following sources:

- Government Documents
- Government Websites
- Research Papers by Other Authors
- Journals
- Articles
- Survey Data

Results and discussion:

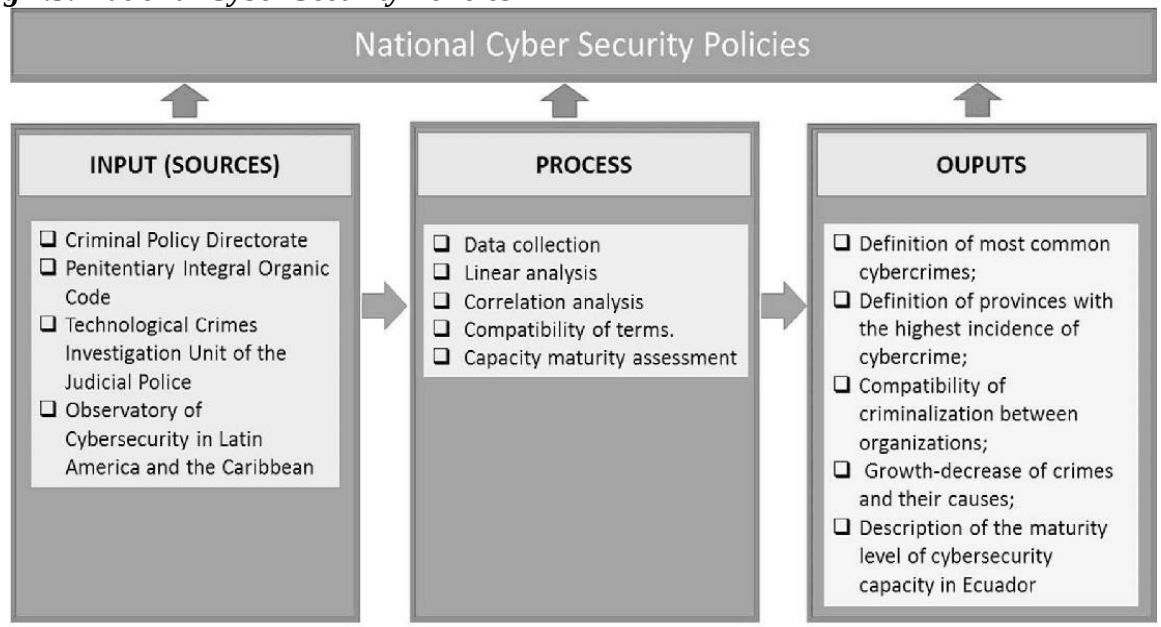
- The IT (Amendment) Act, 2008, diminished the quantum of discipline for a lion's share of cyber wrongdoings. This should be corrected.
- Most of cyber violations should be made non-bailable offenses.
- A complete data assurance system should be joined in the law to make it progressively powerful.
- Parts of Section 66A of the IT Act are past the sensible limitations on the right to speak freely of discourse and articulation under the Constitution of India. These should be evacuated to make the arrangements lawfully feasible.
- The administration should progress in the direction of two-sided collaboration with different nations for trading of data on cyber violations.

Cyber Crimes, in India are registered under three main heads i.e.,

- IT Act
- The IPC (Indian Penal Code)
- State Level Legislations (SLL)

National Cyber Security Policies: In 2013, Ministry of Communication and Information Technology, GoI had discharged the National Cyber Security Policy to ensure data with the target to forestall wholesale fraud, secure budgetary data, abstain from being ransacked and harming of online notoriety, keep up business notoriety, guard client from legitimate proceedings,etc. It diagrams a guide to make a structure for far reaching, synergistic and aggregate reaction to manage the issue of digital security at all levels inside the nation.

Fig 1.5. National Cyber Security Policies



NCS approaches has proposed to set up various bodies to manage different degrees of danger, alongside a national nodal office, to facilitate all issue identified with secure the internet in India. National Critical Information Protection Center (NCIIPC) avoid digital security dangers in key zones, for example, air control, atomic and space.

Vision is to assemble a safe and flexible the internet for residents, business, and government and furthermore to shield anybody from mediating in protection.

Strategic to ensure data and data framework in the internet, manufacture abilities to forestall and react to digital danger, decrease vulnerabilities and limit harm from digital occurrences through a blend of institutional structures, individuals, procedures, innovation, and collaboration.

Conclusion: With expanding traffic in the virtual world, the odds of falling prey to cybercrime pose a potential threat at the same time, more so on account of women who are regularly observed as easy prey. The classes of online wrongdoings focusing on women have extended and the wave has neither disregarded India. A couple of all the more new ages violations that merit a notice here are cyber flares, cyber eve-prodding, and cyber being a tease and cheating. Women in India all things considered avoid announcing matters, dreading potential negative media exposure, which may unsalvageably affect their notorieties. The additional time women spend on the web, without being totally mindful of the entanglements of the web, the more defenseless they become. Women ought to be progressively aware of shield themselves from focused online assaults.

Topic Covered	Description
Digital Crime	An unlawful demonstration where the PC is utilized as an apparatus or target or both.
Reasons for Cyber Crime	Need, Opportunity and Rationalization
Dangers of Cyber Crime	Virus, Malware, DoS, Network related assaults, Remote access
Strategies for Cyber Crime	Cyber Stalking, Domain Names, Cyber Squatting, Cyber Extortion, Cyber Cheating, Cyber Warfare, Cyber Terrorism, Phishing and Vishing

Table 1.7: Description of topic Covered

Correlation with ancient Indian literature: We as a whole know that in our life innovation assumes significant job. It is a major impetus being developed and modernization of society. The significance of innovation has been demonstrated not exclusively the present current time yet it is likewise demonstrated in antiquated period like Vedic Era. For instance, still we don't have any responses for the specialized turn of events and advancement of that period like intra-earthly excursion in type of 'Lok-Parilok Bhraman', Prediction of present and future, Medicare of genuine disease, utilizing flying transportation medium as a 'VAHAN', telescope(to see the articles which were exceptionally poor) and so on.

Machine and Robotic Technology: The Vedic Era has a loads of model which shows that around then the innovative advancement had achieved an extraordinary stature. For instance, Pushpak Viman, Crossing the ocean or huge mountain. This innovation demonstrates that they knew about the job of gravity and law of radiating and centripetal power. Because of these information and advancement, individuals were utilizing flying items for voyaging. They were additionally acquainted with the job of erosion so the arrival of flying articles 'Viman' could be protected. The information on material and shape was logical to make the arial made of excursion extremely protected.

In vedic writing, we found the references of talking winged creature i.e, 'Jatayu', creature 'jamvant', 'Ahiravat', and so forth. These is by all accounts like a robot. The buddhistic bhaisajaya vastu cited when a printer went to yavanya nation and visited the home of

yantracharya(teacher of mechanical designing) he met a machine young lady who washed his feet and appeared to be human yet couldn't talk.

Nuclear rocket innovation: The reference of 'Brasmastra' of like innovation shows that it is fundamentally the same as Inter Continental Missile System of the cutting edge time. The impacts of mass obliteration are case of atomic or nuclear bomb. The precision of development of flying item and landing doesn't conceivable without exact numerical estimation which shows the job of PC like framework around then. To control the speed and course of the rocket "Bharmashastra' or other 'bolt' for hitting the objective appropriately, without PC innovative turn of events, it is difficult.

Data Collection and Processing: The references of 'Vimana', Speaking feathered creature and Animals, information on airplane innovation, mechanical highlights shows that the Vedic Era was enhanced with Science and innovation. Concerning colossal Data Collection and Processing, we have genuine case of 'God Chitragupta'. He was dealing with the database of

every single living animal and arranged according to 'Karma'. On that premise, the 'Karmafal' had been chosen. We can envision the greater part of data, its preparing and from there on the resultant. It is like super PC of present day period.

These entire procedures likewise set up that around then Chitragupta had such kind of cutting edge hard circle in which the data of all animals were put away. They had propelled handling office which could separate according to 'karma' precisely.

On the off chance that we contrast the current PC's highlights and Chitragupta's work design, we see that in the present PC, there has been sure limit of memory, restriction of data assortment, constrained asset to change over the data into valuable item, cutoff of different records dealing with and so forth. We are likewise confronting numerous dangers i.e., infections, cyber security or mechanical misrepresentation. In any case, Chitragupta's PC had boundless memory power, separating all data, doing numerous works at same time and finally however not least that there were no danger of an infections or cyber security.

Overseeing Information as data and its transmission: In the cutting edge period, at first the enormous issue was to deal with and store the data as data. After mechanical turn of events and progression of PC, this issue has been settled at enormous degree with the assistance of wire, the data is being transmitted to wanted spot. After advancement of

remote method of transmission like wifi-network, Bluetooth, satellite availability, the speed and precision has been expanded at significant levels.

In Vedic Era, we have numerous references which set up the presence of wire and remote made of transmission. We can envision it in the job of ruler Narad and different Rishis. The Rishis had same strange powers as mantra to transmit the data/data starting with one spot then onto the next. We can envision that at that period the 'God' could transmit and became vanish and show up at wanted spot. These puzzling high transmission innovations are as yet unanswered. The master 'Narda' is otherwise called 'Brahmrishi' which shows that he can move in entire 'Brahmand'.

We have references of Bhagwad Geeta in which it is referenced that at the hour of war of 'Mahabharta' at kurushetra, Sanjay was broadcasting the live editorial to lord Dhrishtrashtra. He was portraying every single exercises of front line progressively. It appears that there was an unequivocal innovation or a satellite availability which made conceivable the existence broadcast of the occurrence continuously. It is extraordinary case of remote made of transmission of data. We can contrast it with the present method of live broadcast .i.e.,

matches, live news, and so forth. It demonstrates nearness of satellite as well as sending or getting transponders, instrument of signs generators, camera which catch the image. Through this, Snjay was depicting live circumstance of Warfield to the King from very spot for example "Hastinapur".

References

1) "Amid spying saga, India unveils cyber security policy". Times of India. INDIA. 3 July 2013. Retrieved 24 September 2013.
2) 'Anti-Cybersquatting Piracy Act (ACPA)', Harvard University. Available at https://cyber.harvard.edu/property00/domain/legislation.html .
3) "For a unified cyber and telecom security policy". The Economic Times. 24 September 2013. Retrieved 24 September 2013.
4) About Cybersquatting', ICANN. Available at https://www.icann.org/resources/pages/cybersquatting-2013- 05-03-en .

5) An introduction to cyber crime and cyber law by R.k. chaubey, second edition, kamala law house, Kolkata
6) Article on cyber crimes by Missouri law house.
7) 'Cybersquatting Cases Up in 2015, Driven by New gTLDs', WIPO, 18th of March 2016. Available at http://www.wipo.int/pressroom/en/articles/2016/article_0003.html .
8) Commentary on Information technology Act,2000 by Apar gupta, second edition, lexis nexis.
9) Criminal law (incorporation of 2012 amendment) by P.S.A pillai, 12th edition, lexis nexis.
10) 'Cybersquatting and Consumer Protection: Ensuring Domain Name Integrity: Hearing Before the Committee on the Judiciary, United States Senate, One Hundred Sixth Congress, First Session, on S. 1255, a Bill to Protect Consumers and Promote Electronic Commerce', United States Congress Senate, General Books, 2011.
11) Dimitrova, M., 'Most Ludicrous Ransomware in 2016', SensorTechForum, 2016. Available at http://sensorstechforum.com/ludicrous-ransomware-2016/ .
12) Finkelstein, W., Sims, J., 'The Intellectual Property Handbook: A Practical Guide for Franchise, Business, and IP Counsel', American Bar Association, 2005.
13) Hlaing, Thit Oo. "Passing off Action on Trade Marks." (2018).
14) "National Cyber Security Policy 2013" (PDF). Department of Information Technology, Ministry of Communications and Information Technology.
15) "National Cyber Security Policy-2013". Department Of Electronics & Information Technology, Government Of India. 1 July 2013. Retrieved 21 November 2014.
16) "National Cyber Security Policy 2013: An Assessment". Institute for Defence Studies and Analyses. 26 August 2013. Retrieved 24 September 2013.
17) 'The Anti-Cybersquatting Consumer Protection Act ("ACPA")', JUX. Available at http://jux.law/the-anti- cybersquatting-consumer-protection-act-acpa/ .
18) 'Trends in Cybersquatting and Internet Domain Names in 2015', WIPO, 17th of March 2016. Available at https://www.youtube.com/watch?v=8v3iua8QZ-8 .
19) 'What is Cybersquatting?', The Anti Abuse Project. Available at http://www.anti-abuse.org/what-is- cybersquatting/ .
20) Yahoo! Inc. vs. Akash Arora & Anr. (1999, February 19). 1999 IIAD Delhi 229, 78 (1999) DLT 285. URL: https://indiankanoon.org/doc/1741869/