INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Dec 2023
ISSN: 2582-6433

CYBER ATTACKS A REAL THREAT

AUTHORED BY: TRIPTI

INTRODUCTION

Cybersecurity is the process of preventing hostile breaches into networks, PCs, servers, mobile devices, electronic systems, and data. Information technology security or electronic information security are common terms used to describe it.[1]

An efficient cybersecurity strategy must have several levels of protection spread across computers, networks, applications, or data that one intends to keep safe. Businesses need to coordinate their technology, people, and policies in order to effectively protect against cyberattacks. A unified threat management system helps speed up the three primary security operations duties of detection, investigation, and remediation. It can also automate integrations across a selection of Cisco Security products.[2]

Cybersecurity is essential because it prevents theft and data destruction of all kinds. This includes data pertaining to intellectual property, personally identifiable information (PII), protected health information (PHI), sensitive information, personal information, and information systems utilized by the public and private sectors.[3]

These days, as the world grows more and more reliant on technology, protecting sensitive data is crucial. Through the theft of financial transactions and personal information, cyber dangers have the ability to impact people all over the world and cause business disruptions. A variety of protocols and techniques that guard computer networks and systems from loss, harm, and unauthorized access are together referred to as cybersecurity. Preventive countermeasures, strong security protocols, and advanced encryption techniques are some of these methods and procedures. By giving cybersecurity first priority, organizations can lower their risk of data breaches, financial losses, and brand damage.[4]

[1] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
[2] https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
[3] https://www.upguard.com/blog/cybersecurity-important
[4] https://www.comptia.org/content/articles/why-is-cybersecurity-important

ISSN: 2582-6433

TYPES OF CYBER ATTACKS

Malware attack- This is one of the most common types of cyberattacks. Trojan horses, worms, spyware, ransomware, adware, and other malicious software viruses are examples of malicious software viruses, or "malware." The trojan virus presents itself as reliable software. Spyware is software that discreetly gathers all of your personal data, while ransomware blocks the network's vital components. The term "adware" refers to the software that displays banner ads and other types of advertising on a user's screen.

Phishing attack- Phishing is among the most well-known and widespread types of cyberattacks. In this type of social engineering attack, the attacker sends the victim fake emails while seeming to be a trustworthy contact. Without recognizing it, the victim opens the email, clicks on the malicious link, or opens the attachment. By doing this, attackers get sensitive data and account credentials. They might also introduce malware through phishing campaigns.

Password attack- In this kind of assault, your password is broken by a hacker utilizing programs and tools like Hashcat, Cain, Abel, John the Ripper, and Aircrack. There are several different types of password attacks, such as dictionary, keylogger, and brute force attacks.

Man-in-the- middle attack- An eavesdropping attack is another name for a Man-in-the-Middle Attack (MITM). In this attack, the attacker hijacks the session between a client and host in order to get in the way of a two-party conversation. Hackers steal and alter data in this way.

SQL injection attack- A Structured Query Language (SQL) injection attack, in which a hacker alters a standard SQL query, can affect a database-driven website. It is carried out by injecting malicious code into a website's open search field, compelling the server to provide crucial information.

Denial of service attack- As a result, the attacker can access, alter, and delete tables from the databases. Attackers could potentially get administrative rights by doing this. A Denial-of-Service Attack puts companies at grave danger. In order to exhaust all of a server's bandwidth and resources, hackers attack servers, networks, and systems by flooding them with requests. As a result, the servers become overburdened with requests, which slows down or crashes the website it hosts. Consequently, the legitimate service requests remain unaddressed.

ISSN: 2582-6433

Crypto jacking- The terms "cryptojacking" and cryptocurrency are closely associated. Cryptojacking is the term for when hackers gain access to someone else's computer with the intention of mining bitcoin. Infecting a website or deceiving the user into clicking on a malicious link are two ways to gain access. They also employ online ads with JavaScript coding for this. Victims are unaware of this because the crypto mining code runs in the background; the only thing they would notice is a delay in the execution.[5]

LAYERS OF CYBER SECURITY

1. Mission critical assets- It is vitally important to secure this data.
2. Data security- When security measures are implemented to safeguard data storage and transit, it is known as data security. To prevent data loss, a backup security mechanism must be implemented, which calls for the usage of encryption and archiving.
3. Endpoint security- This layer of protection ensures that user device endpoints are not compromised. This covers the safeguarding of laptops, desktops, and mobile devices. Depending on a company's demands, endpoint security systems allow for protection on a network or in the cloud.
4. Application Security- This has to do with the security controls that limit who can access a program and how your assets can be accessed by it. It also covers the application's internal security. Applications are typically built with security features that keep users safe even when they are using the app.
5. Network security- Here, security measures are implemented to safeguard the company network. Preventing unwanted access to the network is the aim. It is essential to apply the required security patches, including encryption, to every system on the company network on a regular basis. Disabling unneeded interfaces is always recommended to increase security against potential threats.
6. Perimeter security- This layer of security guarantees that an organization is fully protected by both digital and physical security measures. It consists of devices like firewalls that guard the company network from outside threats.
7. The human layer- The human layer is a crucial component of the security chain, despite being seen as the weakest link. As an example, it integrates phishing simulations and management controls. The goal of these human management controls is to safeguard the

[5] https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

ISSN: 2582-6433

most important security elements for a corporation. This encompasses the very real risk that a firm faces from people, hackers, and hostile users.[6]

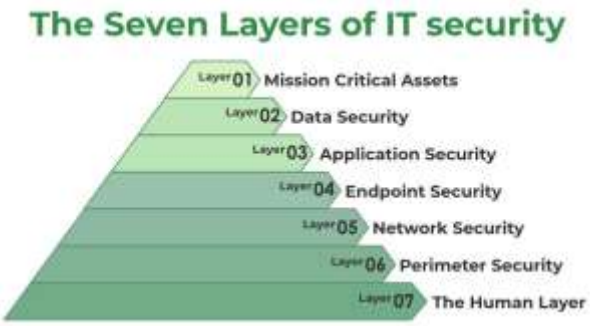

Image credit: Geeks for Geeks

NATIONAL CYBERSECURITY POLICY, 2013

1. The National Cyber Security Policy (NCSP), released by the Indian government in 2013, contained a variety of strategies for fending against cyber security risks.
2. This Policy aims to give people, businesses, and the government access to a trustworthy and safe internet. Additionally, it works to strengthen, monitor, and safeguard cybersecurity defences.
3. This Policy aims to secure the information infrastructure in cyberspace, reduce vulnerabilities, build capacities to prevent and respond to cyberattacks, and limit damage from cyber events using a combination of institutional structures, processes, technology, and cooperation.

Objectives:

1. Here are some major cyber security objectives of the National Cyber Security Policy
2. To provide a secure online environment for the nation, foster proper confidence and trust in IT systems and online transactions, and thereby boost IT use across all economic sectors.
3. To protect information as it is being processed, stored, transported, and handled in order to protect citizen privacy and lessen financial damages from data theft or cybercrime.
4. To strengthen law enforcement capabilities and enable effective cybercrime investigation, prosecution, and prevention through appropriate legislative action.
5. To create infrastructure for assessing and verifying the security of ICT products and

[6] https://microage.ca/cybersecurity-layering-approach/

ISSN: 2582-6433

services in order to increase public knowledge of their integrity.

6. To provide businesses with financial incentives to implement standard operating procedures and security measures.
7. A culture of cyber security and privacy will be fostered through an effective communication and promotion strategy, permitting responsible user behavior and activities.
8. To address the needs of national security by creating suitable indigenous security technologies via commercialization, solution-focused research, and frontier technology research.
9. To offer a framework for assurance in the creation of security policies; additionally, to encourage and facilitate conformity assessment-based actions aimed at achieving compliance with international security standards and best practices.
10. To strengthen the legal framework in order to provide a safe environment for cyberspace.[7]

LEGAL FRAMEWORK IN INDIA

INFORMATION TECHNOLOGY ACT, 2000

Sec 43- Penalty and compensation for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, -

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

[7] https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

ISSN: 2582-6433

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

66. Hacking with computer system.

(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 hack:

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

66B. Punishment for dishonestly receiving stolen computer resource or communication device. –Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.[8]

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource. –Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to

[8] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
66C. Punishment for identity theft. –

ISSN: 2582-6433

three years and shall also be liable to fine which may extend to one lakh rupees.[9]

THE INDIAN PENAL CODE, 1860

464. Making a false document. —A person is said to make a false document or false electronic record—

First. —Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any [electronic signature] on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the [electronic signature], with the intention of causing it to be believed that such document or part of document, electronic record or [electronic signature] was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly.—Who without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with 4 [electronic signature] either by himself or by any other person, whether such person be living or dead at the time of such alteration; or Thirdly.—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his 4 [electronic signature] on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.]

465. Punishment for forgery. —Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

468. Forgery for purpose of cheating. —Whoever commits forgery, intending that the 1 [document or electronic record forged] shall be used for the purpose of cheating, shall

[9] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

ISSN: 2582-6433

be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.[10]

469. Forgery for purpose of harming reputation. —Whoever commits forgery, 2 [intending that the document or electronic record forged] shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

470. Forged document. —A false 3 [document or electronic record] made wholly or in part by forgery is designated "a forged 3 [document or electronic record]".

471. Using as genuine a forged document or electronic record. —Whoever fraudulently or dishonestly uses as genuine any [document or electronic record] which he knows or has reason to believe to be a forged [document or electronic record], shall be punished in the same manner as if he had forged such [document or electronic record].[11]

CASE LAWS

Shreya Singhal v. UOI[12]

In this case, Following the death of a political leader, two ladies were detained under Section 66A of the IT Act for posting comments on Facebook that were deemed indecent and undesirable. The IT Act's Section 66A penalizes anybody who uses a computer resource or communication to disseminate information that is derogatory, inaccurate, or that incites annoyance, discomfort, danger, insult, hatred, hurt, or malice. After the arrest, the women filed a petition alleging that Section 66A of the IT Act violates their right to free speech and expression, thereby making it unconstitutional. There was a challenge to the legality of Section 66A of the IT Act before the Supreme Court. Three ideas served as the foundation for the Supreme Court's ruling: incitement, advocacy, and discussion. It was noted that the essence of freedom of speech and expression is the simple act of debating or even promoting a cause, regardless of how unpopular it may be. It was discovered that Section 66A was capable of limiting all forms of communication and that it

[10] https://www.indiacode.nic.in/bitstream/123456789/2263/1/aA1860-45.pdf
[11] https://www.indiacode.nic.in/bitstream/123456789/2263/1/aA1860-45.pdf
[12] AIR 2015 SC 1523

ISSN: 2582-6433

did not distinguish between inciting public disorder, security, health, or other issues through words that are offensive to some people and merely advocating for or discussing a cause. The Court responded to the inquiry of whether Section 66A seeks to shield people from defamation by stating that it forbids insulting remarks that might irritate a person but do not harm his reputation. Nonetheless, the Court further pointed out that since there was a discernible distinction between material conveyed via the internet and through other channels of communication, Section 66A of the IT Act did not violate Article 14 of the Indian Constitution. Furthermore, the claim of procedural unreasonableness was not even addressed by the Apex Court due to its substantive unconstitutionality.[13]

Avnish Bajaj v. State (NCT) of Delhi[14]

The CEO of Bazee.com, Avnish Bajaj, was detained for transmitting cyber pornography in accordance with Section 67 of the IT Act. Via the bazee.com website, another person had sold copies of a CD that contained sexual material. The Court observed that Mr. Bajaj had no involvement whatsoever in the transmission of any pornographic content. Furthermore, the Bazee.com website did not allow users to view the sexual content. However, Bazee.com is paid for running advertisements on its website and gets a commission from sales. The Court further noted that the information gathered suggests that someone other than Bazee.com is responsible for the cyberpornography offense. Mr. Bajaj was granted bail by the court, contingent upon the provision of two sureties, each worth Rs. 1 lakh. But the onus is on the accused to prove he was only a service provider and didn't create the content.[15]

CBI V. Arif Azim[16]

NRIs were able to send Sony products to their Indian friends and relatives after making an online payment for them through a website named www.sony-sambandh.com.

In May 2002, an individual going by Barbara Campa visited the website and placed an order for a Sony Color TV and a cordless phone for Arif Azim in Noida. After using her credit card to make the payment, Arif Azim received the stated order. But since the actual owner denied making the purchase, the credit card company notified the business that the money was made without

[13] https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
[14] (2008) 105 DRJ 721
[15] https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
[16] 105 DRJ 721

ISSN: 2582-6433

authorization. Consequently, a complaint was filed with the CBI, and a case was also registered in accordance with Sections 418, 419, and 420 of the Indian Penal Code, 1860. According to the findings of the inquiry, Arif Azim obtained Barbara Campa's credit card information while employed at a call center in Noida, which he then exploited. Arif Azim was found guilty by the court, but because he was a young child and this was his first conviction, the court treated him with mercy. The convicted party was discharged by the court to serve a year of probation. This was one of the seminal instances in the field of Cyber Law because it demonstrated how, in situations where the IT Act is insufficient, the Indian Penal Code, 1860 might serve as a useful legal resource.[17]

SMC Pneumatics (India) Pvt. Ltd v. Jogesh Kwatra[18]

Defendant Jogesh Kwatra worked for the plaintiff's business. He began disparaging the company and its managing director, Mr. R K Malhotra, by sending rude, abusive, filthy, and insulting emails to his employers and many subsidiaries of the aforementioned organization across the globe. It was discovered throughout the investigations that the email came from a New Delhi cybercafé. During the investigation, the Cybercafé attendant recognized the defendant. The plaintiff canceled the defendant's services on May 11, 2011. Because the court did not meet the requirements for certified evidence under section 65B of the Indian Evidence Act, the plaintiffs are not entitled to the relief of a perpetual injunction as requested. The court was unable to accept even the strongest evidence since there was no concrete proof that the defendant was the one sending these emails. The defendant was also ordered by the court to refrain from disseminating or publishing any disparaging or abusive content about the plaintiffs online.[19]

CHALLENGES

1. Breach of national security: Cyberattacks are a type of proxy war that have the ability to seriously compromise national security and do extensive damage even in the absence of direct combat. An indirect nuclear conflict could result, for instance, from cyberattacks on nuclear power plants. Serious repercussions for both national money and human life could result from this.
2. Dangerous to financial integrity: The financial systems of more nations are being targeted by cyberattacks. For instance, in 2017, hackers attempted to conduct a $170 million fund

[17] https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
[18] CM APPL. No. 33474 of 2016
[19] https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/

ISSN: 2582-6433

transfer by attacking the Union Bank of India. The financial integrity of the nation may be in jeopardy due to an increase in cyberattacks on Indian financial institutions.

3. Intellectual property rights theft: According to NITI Aayog, cybercriminals are focusing on stealing intellectual property from nations so they can resell it to foreign corporations for hefty profits. This may be data theft pertaining to Indian traditional knowledge.
4. Hacktivism: These are the politically or socially oriented internet demonstrations. It involves mobile apps and devices as well as the cyberattacks that go along with them, causing riots and escalating tensions amongst communities. The Covid-19 epidemic and the Delhi riots are two examples of this.
5. Threat to critical infrastructure: Critical infrastructure, including the electrical grid, banking system, telecommunications, sensitive government websites, air traffic control, etc., has been under attack from China. For instance, China's involvement in the Mumbai blackout was suspected.
6. Data theft: Cybercriminals use ransomware attacks to steal personal data, such as credit card, debit card, and banking information, in order to profit. This has been observed to be a growing phenomenon, with thousands of cyberattacks occurring annually.[20]

CONCLUSION

The IT Act and the Rules enacted under it regulate the Cyber Law system. Additionally, if the IT Act is unable to address a particular kind of offense or if it does not contain comprehensive rules about an offense, one may also turn to the provisions of the Indian Penal Code, 1860.

The Cyber Law system is yet insufficiently capable of handling the variety of Cyber Crimes that are currently being committed, nonetheless. As the nation moves closer to the "Digital India" movement, new types of cybercrimes are continually emerging and becoming part of the cyberlegal system. India's Cyber Law legislation is less robust than those of other countries.

[20] https://unacademy.com/content/upsc/internal-security-notes/indias-challenges-in-cyberspace/#:~:text=India%20is%20the%20third%20most,by%20security%20solutions%20provider%20Symantec.